Disclaimer:
"The content of this Deliverable D2.1 represents the views of the author only and is his/her sole responsibility; it cannot be considered to reflect the views of the European Commission and/or the Consumers, Health, Agriculture and Food Executive Agency or any other body of the European Union. The European Commission and the Agency do not accept any responsibility for use that may be made of the information it contains."

D2.1 WMDA educational webpage on security in organisations providing stem cells.

Grant Agreement number: 837354
Project acronym: SAVDON
Work Package number: WP2

Organisation: **World Marrow Donor Association (WMDA)**
LEAR: Esther Pustjens
Project coordinator: Lydia Foeken
Tel: 0031 88 505 7900
E-mail: lydia.foeken@wmda.info
Organisation website address: www.wmda.info

Co-funded by
the Health Programme
of the European Union

"This Deliverable D2.1 of an activity received funding under an operating grant from the European Union's Health Programme (2014-2020)."

Table of Contents

Security & Privacy Information – General Data Protection Regulation

As medical and genetic information continues to become more valued by cyber criminals, privacy regulators are responding by applying increasing restrictions on the cyber security and cross-border data export protections applied to personal information. As the World Marrow Donor Association (WMDA) community maintains a uniquely large and diverse genetic dataset, this changing landscape presents new risks to WMDA registries and must be managed closely. To support the membership, cyber risk experts within the WMDA have launched a WMDA Security and Privacy Committee (WMDA-SPC; Appendix 1) to assist the WMDA members in cyber risk education and the practical application of cyber risk best practices.

Beginning in the spring 2017, WMDA meetings have included focused sessions on cyber security and data privacy. The inaugural education session at the Marseille meeting overviewed general cyber risk trends while providing general information on the soon-to-be enforced European Union General Data Protection Regulation's (GDPR) operational impacts on EU and non-EU stem cell registries. At the Minneapolis meeting in November 2017, Data Protection Officers from the German, UK, and US registries shared their experiences in bringing their registries towards GDPR compliance. At the request of several session attendees, several reusable GDPR-ready artefacts have been assembled and published on WMDA Share (see Chapter 2. Reusable GDPR artefacts) for other members to adopt and modify to their needs. WMDA members are encouraged to leverage the templates to fast-track or verify their GDPR compliance plans. Additional session(s) on data privacy and information security were organised for the 2018 WMDA meeting in Munich and the 2019 WMDA meeting in Noordwijk. These were designed for all attendees.

The WMDA meetings were focused on education of the WMDA membership on how they could implement the European GDPR in their daily operations. In addition, the WMDA community started to explore how to maintain traceability and if it is feasible to remove the name of the patient in the search process. Based on these meetings three pathways have been developed:

- Change of WMDA Standards to ensure that all WMDA member organisations (that are accredited) work according European data security standards
- Remove patient name from searches (in case the patient has not given consent)
- Develop an infrastructure for data breaches

The WMDA developed standard Data Use Agreements (DUA) that WMDA members could use (Appendix 2, 3 and 4). All Data Use Agreements are signed and available on a WMDA webpage in case a data breach occurs.

A group of ICT specialists worked on educational guidance that helps the WMDA community to start up conversations with IT specialist to comply with the data security standards. The standards were explained during a full day workshop to WMDA members at the WMDA meeting in March 2019. For those, who were not able to attend the meeting a webinar was organised.
In October 2019, the head of Specialist Services IT at NHS Blood and Transplant UK and member of the WMDA Standards Committee gave a webinar about the new IT standards 2020. This also included the GDPR rules for these standards. This webinar is accessible via:

- https://www.youtube.com/watch?v=kEIJUZSPqb8&feature=youtu.be

On WMDA Share, the educational resources on data protection and security for security officers submitting patient, donor and cord blood data for international research are display on the page **Security & Privacy Information (including GDPR)**. This page is accessible for the WMDA Community.

Due to the GDPR rules, WMDA cannot give everyone access to these webpages. The information on there in strictly for the WMDA community. Therefore, below are screenshots to show the outline of this website.

The home page looks as follows:

The topics on the page cover:

- WMDA Data Use Agreements
- Reusable GDPR artefacts
- Top Misunderstandings of the General Data Protection Regulation (GDPR)
- WMDA Policy & Procedures against recent Cyber Security threats
- Written Information Security Policies - Table of content examples

1. WMDA Data Use Agreements

1. WMDA Data Use Agreements

- WMDA Spring meeting 2017: WMDA Cyber Risk Management
- WMDA Fall meeting 2017: General Data Protection regulation (GDPR) Overview

Based on the workshops in 2017, the WMDA has decided to assist the membership in the implementation of the GDPR.

Find here three appendices that have contributed to perform international exchange of data.

- Registry-to-Registry Data Use Agreement (DUA)
- WMDA - DUA Explanatory Information
- WMDA - DUA

2. Reusable GDPR artefacts

- GDPR-ready third party data processing contract clauses
- GDPR-ready donor consent agreement template
- GDPR-ready website privacy policy for donors
- GDPR readiness assessment tracking tool

3. Top Misunderstandings of the General Data Protection Regulation

3. Top Misunderstandings of the General Data Protection Regulation (GDPR)

1. My registry is located outside of the European Union. GDPR does not apply.

Fact - GDPR applies to any organization that receives personal information of a European resident, no matter where the organization is located or where the European resident is located. Since stem cell supply chains traverse the globe, it is likely that all registries accepting European donors are processing personal data of European residents and impacted by GDPR.

2. My registry doesn't collect personal data from any European resident. GDPR does not apply.

Fact - One major change of the new GDPR from the previous EU Privacy Directive is the obligations it imposes on third party and foreign data processors. While the expanded donor consent requirements are limited to the registries that directly collect personal information and biological sample from the donor, foreign registries will need to meet specific security requirements (enforced by contract) before the European registry can share their donors' data. Non-European registries should ensure their able to comply with these requirements to avoid disruption in their ability to receive EU personal data. Additional data export/import requirements may apply to registries where the European Union has deemed certain countries to have inadequate privacy laws.

3. The personal data my registry receives is de-identified. GDPR does not apply.

Fact - The GDPR has broadly defined Personal Data as "any information relating to an identified or identifiable natural person." GDPR makes it clear that personal data that is linkable through one or more factors, such as through a unique Donor ID number, remains within the GDPR jurisdiction. While the donor and patient personal attributes must be minimized (formally called pseudonimization), the remaining donor record remains linkable. Consequently, registries that receive minimized donor records from European registries are not exempt from the regulation.

4. Hackers don't care about this type of data.

Fact - Hackers are finding new and creative ways to monetize medical information for short-term financial gain or long-term national strategic advantages. The volume and diversity of the WMDA donor inventory could present a unique opportunity to motivated cyber criminals. The WMDA community is responsible for providing adequate cyber defenses and data governance to protect the personal information entrusted to us and ensure the long-term sustainability of cross-border cell transplants.

4. WMDA Policy & Procedures against recent Cyber Security threats

4. WMDA Policy & Procedures against recent Cyber Security threats

WMDA is always aware of the vulnerable data that we host for all our organisational members as well as the personal data from our members. When larger cyber security treats have been identified, we will publish on this page what we, as WMDA, are scheduling to do or have done to minimize the risk to our systems and your data. In the near future, we will outsource these activities by a certified company that will maintain our network and infrastructure.

4.1 Meltdown and Spectre

What is the issue

- A newly discovered form of cyber security threat is being reported.
- This threat allows attackers to exploit common features of microprocessors.
- The affected systems are being used in about all devices, including pc's, servers, laptops, tablets, smartphones, and other gadgets.
- These threats are known as "Meltdown" and "Spectre", and can be (partially) addressed by applying updates.
- Not all systems will have updates, or have updates available yet.

What is doing WMDA

We have set up a mitigation plan that involves

- A careful inventory and analysis of the systems affected, including 3rd party (cloud based) providers
- Assessing the level of vulnerability
- Checking the availability of patches and updates on firmware, operating system and software level.
- Schedule the mitigation actions to be taken.

What can you do?

- Inform yourself about the issue. https://meltdownattack.com/
- Contact your IT staff to know how this may affect you, and what are best practices
- On your own devices : apply all available patches and updates, including operating system, updates from your hardware manufacturer, and browsers as soon as they come available
- On your own network : switch your DNS to a service that blocks malware on the network, eg quad9.net
- In your own browser : install an adblocker in your browser, eg "uBlock Origin"
- Always inform and consult your IT staff to see if these measures apply to you.

5. Written Information Security Policies - Table of content examples

5. Written Information Security Policies - Table of content examples

- Australian draft policy
- Example of Australian University
- Example of table of contents from different size of registries
- Example of NMDP

Appendix 1. WMDA Security and Privacy Committee

The purpose of the WMDA Security and Privacy Committee is to encourage and enable the WMDA and its members in managing information security and privacy matters as a global business risk. With proper risk management, WMDA can ensure the long-term sustainability of global data sharing that is necessary to achieve the WMDA mission.

The WMDA Security and Privacy Committee (WMDA-SPC) will achieve this purpose by:

- Establishing minimum security and privacy standards that are required for WMDA membership
- Supporting the WMDA Accreditation process to ensure these standards are enforced
- Providing regular education and training to members at semi-annual meetings and with publications
- Informing members on emerging risks and regulations that may threaten the WMDA mission
- Providing practical guidance specifically crafted for small- and mid-sized stem cell registries with an international supply chain and data profile

Current projects

1. **DUA Agreements.** WMDA-SPC will assist WMDA and members in establishing and socializing WMDA/Registry and Registry-to-Registry GDPR compliant DUAs. This includes reconsiderations of a hub-style registry-to-registry agreement to achieve the requirements of GDPR.
2. **Incident Ledger on WMDA Share.** WMDA-SPC will create, maintain and socialize a ledger of data privacy and security incidents encountered by WMDA members. These incidents will be published on WMDA Share. All aspects of any incident will be anonymized, including WMDA member identifying information. These real incidents will be used as educational materials (lessons learned) to improve the overall security of the WMDA network.
3. **WMDA Security Standards.** WMDA-SPC will assist with the finalisation, education and socialisation of the new security standards and guidelines.
4. **Peer Security Assessment / Accreditation.** WMDA-SPC will establish a simple, scalable and repeatable assessment process to perform registry-to-registry peer risk assessments of registry applications. One security, privacy, or IT representative from WMDA would perform a security and privacy assessment on behalf of the entire WMDA network. Basic information on the results, and any material corrective actions, will be published on WMDA Share. Members may rely on these results to comply with their own internal and external risk assessment requirements. Large registries and Bone Marrow Donors Worldwide (BMDW) would be the early adopters of this new process. (This process was piloted between NMDP and ZKRD in June 2018).
5. **EMDIS Security and Privacy / Global Erasure Request.** WMDA SPC-will review, define and document technical security and privacy specifications for the future enhancement of EMDIS. The updates would formally incorporate privacy-by-design principles in addition to modern security specifications (encryption, authentication, etc). The current EMDIS specifications share unnecessary privacy data (e.g., DoB) that make it difficult for members to meet global privacy obligations.
6. Participate in the Substances of Human Origin (**SoHO**) Expert Group

Appendix 2. Registry-to-Registry Data Use Agreement

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:

(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;

[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.

(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 [date], [city/town],

Name of the organisation:
Address:
Tel:
Fax:
E-mail:
Other information needed to identify the organisation:

On behalf of the organisation:
Name (written out in full):
Position:
Address:
Other information necessary in order for the contract to be binding (if any):

(stamp of organisation) (signature)

Appendix 3. WMDA – DUA Explanatory Information

Explanatory information on Data Use Agreements (DUAs) for WMDA Registries

NOTE: This explanation is focused on the European Union (EU) privacy obligations in establishing inter-organisational privacy agreements (i.e., Data Use Agreements (DUA)). However, while this information emphasizes specific EU requirements and expectations, the need for a similar agreement is common across most international legal jurisdictions.

The EU privacy regulation (GDPR) is more verbose on the contractual terms of the DUA, compared with other similar international regulations. As WMDA processes data on behalf of many global registries and is domiciled in the European Economic Area, WMDA has chosen to align its DUA to comply with GDPR to ensure an acceptable global standard for all of its members.

EXECUTIVE SUMMARY

A new EU privacy law, the General Data Protection Regulation (GDPR), is set to replace the prior EU Data Protection Directive 95/46/ec, effective May 25, 2018. GDPR establishes a harmonized set of privacy obligations for the "processing" (performance of any "operation" on personal data, for example collection, organisation, storage, alteration, or use) of the personal data of European residents. With regard to third party data processing of personal data, GDPR expands significantly upon an organisation's responsibility for overseeing its third party processing activities and sets out specific rules for allocating responsibility between the organization and its third party data processors. All WMDA member organisations that collect or process European personal data will likely need to take action.

GDPR Article 28 requires that organisations must only use third party processors that can provide "sufficient guarantees" in ensuring the protection of the privacy and rights of the data subject. The processing directives between the organisation and its third party processors must be governed by a binding contract. These contracts must direct and control the purpose of processing, onward sharing of data, data subject rights, and other privacy and security obligations, to allow the controller's purpose to be achieved while also protecting the privacy rights and freedoms of the data subject. This contract between an organisation and its third party processors is commonly called a Data Use Agreement (DUA). The DUA must be in place and executed directly between two legal entities sharing European personal data. As noted above, most countries have a similar principle in their respective privacy regulations.

International stem cell registries have, at a minimum, two primary data sharing arrangements that must be governed by the DUA described above. First, any registry listing its donors and/or cord blood units with WMDA, or receiving personal data via WMDA, will need to execute a Registry-WMDA DUA. Further, any registry that is sharing or receiving personal data directly from another registry, outside of WMDA, will likely require a Registry-Registry DUA. A template of a Registry-Registry DUA is available for WMDA members through WMDA Share. These WMDA-issued DUAs have been reviewed and approved by legal counsel and determined to contain the necessary information to comply with the DUA obligations of

GDPR. Some registries may also be using sub-processors (e.g., IT service providers) as part of their operations to process European personal data. As the sub-processing arrangements require similar guarantees and legal agreements, registries may feel compelled to inventory any sub-processing and reassess their vendor agreements to achieve compliance.

INTERNATIONAL TRANSFERS OF PERSONAL DATA

In general, European personal data can be transferred to a third country only if certain conditions are met by both the controller and processor. These conditions include: the third country has achieved an "adequacy" designation (Art. 45); the organization has taken upon themselves to provide "appropriate safeguards" (Art. 46); or the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks (Art. 49.1.a). As of this writing, the European Commission has so far recognized Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US (limited to the Privacy Shield framework) as providing adequate protection.

As many WMDA registries are not in a country with an adequacy designation, the DUA templates provided by WMDA rely either on consent, or on the declaration of appropriate safeguards – specifically through a set of Standard Contractual Clauses preapproved by the European Commission. These terms allow for the lawful export of European personal data in the scenarios where the third-countries do not have an adequacy designation.

NEXT STEPS

Today, you received a copy of the Data Use Agreement between WMDA and the listing entities together with this information. You do not have to sign this copy. Next week, we will send out the official Data Use Agreement by using DocuSign to collect your signature.

Disclaimer: This information and the commentary contained in it are not legal advice. GDPR is a complex principle-based law which is open to interpretation and also contains numerous areas where Member States are permitted to include additional requirements to the core GDPR requirements. There is currently very limited guidance and commentary on Article 28 GDPR, and supervisory authorities and courts may take different views to those expressed here. GDPR also creates significant compliance risk introducing fines of up to 4% of annual worldwide turnover for the most serious breaches, as well as the risk of private claims by data subjects for compensation. It is strongly recommended that organisations seek legal advice on how to prepare for GDPR, including in relation to the contractual relationships between data processors and data controllers.

Appendix 4. WMDA – DUA

DATA TRANSMISSION AND USE AGREEMENT

This Data Transmission and Use Agreement ("**Agreement**") is entered into by and between

World Marrow Donor Association
(henceforth called "**WMDA**"),
a non-profit association established under Dutch law,

and

ORGANISATION NAME

+ address
(henceforth called "**Listing Entity**"),

each a "**Party**" and collectively the "**Parties**".

The Effective Date is the date of the final signature of the Party executing this Agreement.

Whereas, on behalf of the Listing Entity, WMDA has created and operates a searchable database of adult donors and cord blood units available for use in hematopoietic stem cell transplantation, which has been established to build, provide, maintain, and optimise an environment with centralised data on human leucocyte antigen ("**HLA**") phenotypes and other relevant data of volunteer stem cell donors and cryopreserved cord blood units ("**CBUs**") and make these data accessible to the other Listing Entities, healthcare professionals (e.g. transplant centre physicians, search coordinators) worldwide that search for a potential match for their patient; and

Whereas, the Bone Marrow Donors Worldwide (**"BMDW"**) has now merged with WMDA and BMDW is now a service provided by WMDA on behalf of the Listing Entity and is called: Search & Match Service; and

Whereas, Listing Entity is a member of the WMDA; and

Whereas, Listing Entity lists with WMDA a file of volunteer stem cell donors and/or, as applicable, volunteer-donated cryopreserved CBUs for international search; and

Whereas, Listing Entity provides WMDA with searching patients ("**Patient**") data; and

Whereas, 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**" herein;

Whereas, the Listing Entity wishes to provide WMDA with relevant data, information, and other records relating to Patients, Donors, and CBUs ("**Data**") necessary to coordinate certain donor product search,

collection and transplant activities. Therefore, WMDA will have access to pseudonymised personal data within the meaning of the General Data Protection Regulation (EU) 2016/679) (hereinafter referred to as '**Personal Data**' and '**GDPR**', respectively); and

Whereas, with regard to the Data, the Listing Entity is the data controller within the meaning of GDPR and WMDA is the data processor. WMDA's operations are limited to processing Data in accordance with the Listing Entity's written instructions unless required to do so by law without having control over the purpose of and means for processing the Data. WMDA 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. Consequently, WMDA merely provides the Search & Match Service on behalf of the Listing Entity and processes the Data on behalf of the Listing Entity in accordance with WMDA's mission and vision as agreed to by the Listing Entity.

Whereas, WMDA recognises the importance of protecting the privacy and confidentiality of Data exchanged to maintain the confidence and trust of Donors, Patients and regulators; and

Whereas, the Parties intend for this Agreement to govern the exchange of Data from the Listing Entity to WMDA and to establish inter alia the obligations of WMDA regarding the use, maintenance, confidentiality, transmission and security of the Data and wish to lay down their arrangements concerning the processing of Data by WMDA in this Agreement.

Now, therefore, the Parties have agreed to be bound by the provisions set forth below:

4. Compliance with Privacy Law

1.1. The Listing Entity 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 its respective applicable laws governing the collection, storage, use, disclosure and access to personal and health information ("**Privacy Law"**). The Parties will co-operate as reasonably required to facilitate compliance with applicable Privacy Law by each Party.

1.2. WMDA undertakes in respect of the Listing Entity to do all that is required of a processor of Personal Data based on the provisions of, or made pursuant to, the GDPR.

5. Scope of Data Exchanged

2.1. Unless otherwise agreed by the Parties, Data exchange will be limited to data elements required for the performing and/or improving processes supporting search, matching, stem cell transplantation and quality assurance. WMDA makes the Data visible to other Listing Entities through 1) interactive user access with the Search & Match Service, on request of a Listing Entity and after approval of the Listing Entities 2) full and/or partial download of the dataset and derived statistics, or 3) application programming interface (API). Healthcare affiliated professionals with bonafide need to search for international donors can only access the Data through interactive user access with the Search & Match Service. The Listing Entity ensures that the Data it exchanges will be in a form that does not enable other persons to identify the

individual to whom the data relates unless necessary to confirm Patient identity or evaluating the match of a Donor. Listing Entity agrees to comply with all Data submission and exchange requirements necessary for the WMDA to provide the Search and Match Service, as amended from time to time. Such requirements will be published by WMDA on its membership website (WMDA Share).

2.2. WMDA will process pseudonymised Personal Data from Donors and Patients 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. A specification of the Data that WMDA can process is available on WMDA membership website (WMDA Share see https://share.wmda.info/x/HYDVCQ) and is based on definition files which will be revised annually by the Listing Entities.

6. Assurances by Listing Entity

3.1 The Listing Entity 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 WMDA of any material change in status under applicable laws.

3.2. The Listing Entity 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 HSC search and transplant procedures, operation of a Listing Entity, quality assurance purposes, and publication of organisation and search activity ("**Purposes**").

3.3. The Listing Entity represents and warrants that the informed and explicit consent from the Donors and Patients of which Data are required has been obtained directly or by its responsible cooperation partner under its respective governing laws (including the GDPR, as applicable) to provide the Data to WMDA for the operation of the Search & Match Service for the Purposes.

7. Processing of Data by WMDA on instruction of Listing Entity

4.1. WMDA will only process (inter alia access, use, share or export) Data received from the Listing Entity at the Listing Entity's written instructions solely for the operation of the Search & Match Service for the Purposes and as provided in this Agreement.

Purposes

4.2. The Purposes are set by the Listing Entity and WMDA is not entitled to make any decisions concerning the purposes of the Search & Match Service.

Required data fields

4.3. The Listing Entity decides what optional Data is supplied by the Listing Entity and is thus included in the Search & Match Service.

Data quality assurance

4.4 The Listing Entity is responsible for the quality of the Data provided to WMDA. On behalf of the Listing Entity, WMDA will validate the quality of the Data as part of the processing procedure and make a processing report and benchmarking / statistical information regarding data quality available to the Listing Entity.

Disclosure to third parties

4.5. On behalf of the Listing Entity, WMDA will disclose Data to third parties for the Purposes and in accordance with the requirements set forth herein. On behalf of the Listing Entity the Data in the Search & Match Service will be shared with:

- Staff members of WMDA member organisations to search for international donors and obtain Data from the Search & Match Service;
- Healthcare affiliated professionals with bonafide need to search for international donors and obtain Data from the Search & Match Service;
- IT service providers maintaining and developing the Search & Match Service;
- Matching programme providers;
- WMDA office staff, as described in clause 5.5.

(the "**Users**")

The WMDA bylaws define the membership categories. The WMDA website outlines the criteria to list and to access to the Search & Match Service.

4.6. On behalf of the Listing Entity, WMDA may provide a full or partial copy of the donor/cord blood file of the Listing Entity or API access to WMDA member organisations that comply to the WMDA Standards and have implemented the measures as described in clause 5.1 in this agreement. In addition, on behalf of the Listing Entity, WMDA may provide healthcare affiliated professionals with bonafide need to obtain limited Data from the Search & Match Service by minimum role-based access to the Search & Match Service and the Data obtained therein.

4.7. Who may become a WMDA member is inter alia laid down on the WMDA website (www.wmda.info) . On behalf of the Listing Entity WMDA may reject or approve an application for a membership. WMDA is not entitled to make any decisions with regard to extending the categories of users of the Search & Match Service to other categories of users.

Summary of Data and internal studies by WMDA

4.8. On behalf of the Listing Entity, the Data provided by the Listing Entity and the search activity related thereto may be summarized and published in the WMDA global trends report which will be made available to WMDA members for their internal use, may be published to the World Health Organization, and may be placed on the WMDA website. Information made available to the WMDA membership or national or international (e.g. EU, WHO) authorities may identify

individual countries or Listing Entities. Information to the general public will in general not identify individual countries or Listing Entities.

4.9. On behalf of the Listing Entity, WMDA may use non-identifying Data for purposes of internal studies, analysis and presentation to improve the Search & Match Service or to advance understanding in blood and marrow transplant. Any external publication will require permission of the Listing Entity.

Use by others

4.10 On instruction of the Listing Entity, WMDA will have in place a policy limiting third-party use, publication, or reproduction of any Data provided by Listing Entity except with the advice from the science committee, and the consent from the Listing Entity.

4.11 A systematic analysis and external publication of the Data of the Listing Entity may only be done on instruction of the Listing Entity. This applies to all form of publication (printed, electronic or other). It also applies to analyses where Data are systematically pooled for analysis (e.g., by country or region) or by overviews showing or comparing several or all Listing Entities.

Sub-processor

4.12 Listing Entity authorises WMDA to engage another processor to process the Data. In the event that WMDA chooses to make any changes to its sub-processors, WMDA will provide a 60-day written notice to all Listing Entities of the change. Should a Listing Entity object to the change, the Listing Entity will have the right to opt-out or de-list their Data. WMDA must enter into an agreement with the applicable third party that covers the same obligations, in particular the obligations that are stipulated in clause 5.1 of this Agreement and which meet the requirements of Article 28 of the GDPR, and offer at least the same level of protection for the Personal Data as this Agreement. As between the Listing Entity and the WMDA, the WMDA shall remain fully liable for the all acts and omissions of any sub-processor appointed by the WMDA pursuant to this clause 4.12. A list of approved sub-processors is provided in Appendix 1 from this Agreement.

Listing Entity's prior consent

4.13 WMDA may not provide Data to other than those described in this Agreement, unless the Listing Entity has given its documented instructions to that end.

8. Technical and organisational measures

5.1. WMDA 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. Said measures will cover, among others, as appropriate:

- The pseudonymisation of all personal data stored;
- The encryption of all personal data in transfer to external systems;

- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;
- Compliance with the WMDA security standards, including (1) the adoption of a credible security framework (e.g., ISO 27001), and (2) ongoing oversight of WMDA's cyber risk by WMDA's highest governance committee.
- Independent penetration testing should be performed annually on all internet facing web applications which process pseudonymised or identifiable Data. Any identified security vulnerabilities must have a documented remediation plan. Risks identified by this testing must be formally overseen by the Data Protection Officer of the WMDA.

5.2. Bearing in mind the state of the art and the costs of implementation, the security measures within the meaning of clause 5.1 must offer an appropriate level of security relative to the risks associated with the processing and the nature of the Data to be protected. Said measures are aimed, in part, at preventing unnecessary collection and further processing of Personal Data.

5.3. The security measures to be taken by WMDA are based on a risk analysis and will cover the risks to such an extent that the reliability requirements are met. The higher the required reliability and/or the required level of security are, the more numerous and stringent security measures WMDA will take to cover the risks present and to actually guarantee the required level of security.

5.4. WMDA undertakes in respect of the Listing Entity to maintain the level of its technical and organisational measures, to improve and refine them where possible, and to modify them to meet the evolving technological and societal developments. To that end, WMDA will monitor the most recent developments and take additional measures insofar as it may reasonably be expected to do so. Upon the Listing Entity's request, no more than annually, WMDA will provide evidence that management oversight has occurred. Such evidence should briefly describe the oversight process, indicate whether WMDA's controls remains aligned to industry best practices, and include a signature of a WMDA board member.

5.5. WMDA 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 names of the WMDA staff members and authorized representatives who will have access to the Data are available on request. WMDA will ensure that unauthorized personnel do not have access to the Data and/or the data processing applications. WMDA certifies that all members of staff authorised by WMDA to access the Data are obliged to observe confidentiality in respect of the Data of which they become aware. To that end, WMDA will have the staff members and authorized representatives in question sign a confidentiality agreement, insofar as it has not already made provisions for this.

5.6. WMDA 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 clauses 4.5 – 4.7.

5.7. The Listing Entity will establish periodically, or whenever circumstances so dictate, whether the technical and organisational measures taken by WMDA still offer an appropriate level of security. With regard to changes made to the services provided by WMDA, the Listing Entity will determine whether the arrangements made are still sufficient and it will ensure that the security requirements are still met after the changes have been implemented.

5.8 Information and audit rights of the Listing Entity only arise under section 5.7 to the extent that the supplied documentation does not otherwise give the information meeting the relevant requirements of the GDPR.

6. Demonstrating compliance

6.1. WMDA makes available to the Listing Entity information necessary to demonstrate compliance with the obligations laid down in this Agreement and allow for and contribute to audits, including inspections, conducted by the Listing Entity or another auditor mandated by the Listing Entity. WMDA will report to the Listing Entity annually about the measures taken and the procedures implemented. All records of any type relating to WMDA's performance of its obligations under this Agreement will be retained by WMDA for the term of this Agreement and no less than three years thereafter, or for a greater period as required by applicable laws. This provision will survive termination of this Agreement.

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

6.3. WMDA will assist the Listing Entity at all times to meet the obligations pursuant to the GDPR. More specifically WMDA will assist the Listing Entity 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. WMDA will promptly, and in any case, within 5 days, notify the Listing Entity 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 Party's obligations under GDPR in respect of the Personal Data.

6.4. WMDA will assist the Listing Entity 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. The security of Personal Data covers, amongst others, the security of processing and the notification of a Personal Data breach to the supervisory authority and Listing Entity.

7 Breach Notification

7.1. WMDA will report any incident in regard to security and Personal Data breaches without undue delay, and in any case within 36 hours, to the Listing Entity, such report to include all information reasonably required by the Listing Entity to comply with its obligations under the GDPR.

7.2. If WMDA 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, WMDA will consult with the Listing Entity and follow any of the Listing Entity's instructions. WMDA will keep the Listing Entity 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 Listing Entity, WMDA will cooperate with Listing Entity in properly informing the data subjects.

8 Cooperation with Supervisory Authorities

8.1. If a supervisory authority is appointed for the Listing Entity under or pursuant to the law, said supervisory authority will at all times be entitled to conduct or commission an audit at WMDA to verify the performance of the Agreement and/or other agreements concluded between the Listing Entity and WMDA. For purposes of said audit, the supervisory authority is authorised, among other things, to request and inspect the information exchanged between the Parties – which explicitly includes emails and other communications between the Parties – and other relevant documents. WMDA will provide its full cooperation in such an audit.

8.2. WMDA will cooperate, on request, with the supervisory authority in the performance of its tasks.

9 Term and Termination

9.1. Term

This agreement will commence on the date of its signature and will continue unless terminated earlier by either Party as provided below.

9.2. Termination

i. Listing Entity will be entitled to terminate this Agreement at any time in writing to the WMDA with immediate effect if the WMDA terminates its activities (including the closure of the WMDA).
ii. Listing Entity may terminate this Agreement on sixty (60) days' prior written notice.
iii. WMDA may terminate this Agreement if the Listing Entity no longer has a membership status with WMDA.

On termination of this Agreement, WMDA must return to the Listing Entity or dispose of, in accordance with the Listing Entity's written instructions, all confidential Personal Data of the Listing Entity and any other Data provided by the Listing Entity pursuant to this Agreement, unless Union or Member State law requires storage of the Personal Data. Representations and obligations to preserve the confidentiality of Data will survive the termination of this Agreement. The Parties must delete or destroy all confidential information in Party's possession within

fifteen (15) days of Agreement termination, or upon the request of the data controller using commercially acceptable methods.

10. Data Transfers to Non-EU Countries

10.1. On behalf of the Listing Entity, WMDA may process Data outside the European Union ("EU" or "Union") for the operation of the Search & Match Service 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.

10.2. In the absence of an adequacy decision by the European Commission (which allows the free flow of Personal Data from the European Economic Area ("EEA") to designated countries, without having to implement any additional safeguards) and of EU standard contractual clauses ensuring such adequate safeguards for Personal Data transferred from the EEA to countries outside the EEA, the Listing Entity represents and warrants that it has obtained the informed and explicit consent, as applicable privacy regulations dictate, from the Donors and Patients of which it collects Data (after the Donors and Patients have been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards) for the transfer of Data by WMDA to WMDA members and users from the Search & Match Service located outside the EEA, as defined in clause 4.5. This, in order to cover the transfer of Data from WMDA as data processor to the Users located outside the EEA.

11 Choice of law and forum

11.1. This agreement is governed by the laws of the Netherlands.

11.2. Any dispute related to this Agreement, whether contractual or arising from unlawful act, must be exclusively brought before the courts of The Hague in the Netherlands.

World Marrow Donor Association	Listing Entity
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

APPENDIX 1: APPROVED SUB-PROCESSORS

Name	Location	Processing purpose
Leaseweb	Amsterdam, The Netherlands	Hosting
Damecon	Rotterdam, The Netherlands	Service provider for private rack at Leaseweb
OptiMaS	Ulm, Germany	Matching Service Provider
Be The Match/NMDP	Minneapolis, USA	Matching patients in internal system
ZKRD	Ulm, Germany	Matching patients in internal system
Gift of Life	Boca Raton, USA	Matching patients in internal system
France Greffe de Moelle Registry - FGM	Saint-Denis La Plaine Cedex, France	Matching patients in internal system
Italian Bone Marrow Donor Registry	Genoa, Italy	Matching patients in internal system