DATA USE AND PROCESSING POLICY

The following Data Use and Processing Policy describing the data use and processing requirements between National Marrow Donor Program ("NMDP") and Center, each a "Party" and collectively, the "Parties") reflects the arrangements that they have agreed to put in place pertaining to the Parties' data privacy and security obligations in performing their respective responsibilities in facilitating the sharing of Personal information between the Parties.

As such, the Parties agree to share Personal Information with each other and agree to use Personal Information according to the terms set out herein.

1. **Definitions**. For purposes of Center's compliance, as applicable, with the following data processing requirements, the following terms have the following meanings. All other terms not defined herein shall have the meaning given to them as set forth in the General Data Protection Regulation ((EU) 2016/679) ("**GDPR**").

   Centers: Transplant centers, collection centers, apheresis centers, cord blood banks, donor centers, recruitment groups, and cooperative registries (each a "Center").

   Data Controller: The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of Personal Data; where the purposes and means of processing are determined by European Union (EU) or Member State laws, the controller may be designated by those laws.

   Data Processor: A natural or legal person, public authority, agency or any other body which processes Personal Data on behalf of the controller.

   Data Protection Legislation: All applicable legislation protecting the Personal Data of natural persons, including: (i) the Data Protection Act 1998; (ii) GDPR; and (iii) any successor legislation to the GDPR or the Data Protection Act 1998, together with binding guidance and codes of practice issued from time to time by relevant supervisory authorities.

   Personal Data: Any information relating to an identified or identifiable natural person ("Data Subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Personal Data shall include special category data, where applicable, as that term is defined in GDPR.

   Processing: Any operation or set of operations performed upon Personal Data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

   Standard Contractual Clauses: The contractual clauses set out in Schedule 3, amended as indicated in that Schedule.

   Restricted Transfer: Any transfer of Personal Data that would be prohibited by the Data Protection Legislation in the absence of the Standard Contractual Clauses.

   EEA: European Economic Area. The EEA includes EU countries and also Iceland, Liechtenstein and Norway.

2. Overarching Data Protection Requirements.

2.1 Internal Procedures. NMDP and Center (each a "Party" and collectively "the Parties") mutually agree to implement administrative, physical, and technical safeguards to protect Personal Data that are no less rigorous than accepted industry best practices, including the International Organization for Standardization's standards: ISO/IEC 27001:2013 (or any successor) – Information Security Management Systems, and shall ensure that all such safeguards, including the manner in which Personal Data is collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions outlined herein.

2.2 Quality Assurance and Ethical Review. Each Party represents that it has obtained all necessary ethical review, consent and governmental approval required under its respective governing laws for donors and patients to participate in the exchange of Personal Data for quality assurance purposes and publication of outcomes.

2.3 Compliance with Data Protection Legislation. Both Parties will comply with all applicable requirements of the Data Protection Legislation and ensure that any of their staff involved with the activities herein shall comply. This clause is in addition to, and does not relieve, remove or replace, a Party's obligations under the Data Protection Legislation.

2.4 Standard Contractual Clauses for Data Transfers to Non-EU Countries. The European Commission has adopted a decision setting out standard contractual clauses ensuring adequate safeguards for Personal Data transferred from the EU to countries outside the EU. The decision obligates Member States to require that companies or organizations using such standard clauses in contracts concerning Personal Data transfers to countries outside the EU are offering "adequate protection" to the data. The EU's data protection Directive (95/46/EC) requires all Personal Data transferred to countries outside the EU to benefit from "adequate protection". The standard contractual clauses offer companies and organizations a straightforward means of complying with their obligation to ensure "adequate protection" for Personal Data transferred to countries outside the EU which have not been recognized by the European Commission as providing adequate protection for such data. Accordingly, the Parties agree that the standard contractual clauses ("EU Standard Contractual Clauses"), included as Schedule 3 herein will apply and govern, only as applicable, when the Data Subject is in the EU.

2.5 Audit. Each Party agrees that the other Party has the right to audit its activities if required by the other Party. Each Party also agrees that the competent authority or authorities of the other Party has the right to inspect its activities, including on-site inspections, should it wish to do so as part of its inspection of the other Party; provided, however, that information and audit rights of the Data Controller only arise under this section to the extent that the Data Processor does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, Article 28(3)(h) of the GDPR).

3. Data Owner Classifications and Respective Responsibilities.

3.1 Data Controller and Data Processor Determination. The Parties acknowledge that for the purposes of the Data Protection Legislation NMDP is the Data Controller and Center is the Data Processor when Center provides services to NMDP and Center is the Data Controller and NMDP is the Data Processor when NMDP provides services to Center. Schedule 2 sets out the Data Controller's directive on the scope, nature and purpose of processing, the duration of the processing, the types of Personal Data and the categories of Data Subjects.

3.2 Data Controller Responsibilities. The Party acting as Data Controller shall:

(a) ensure that it has all necessary appropriate consents and notices in place to lawfully collect, process and transfer Personal Data to the Party acting as Data Processor for the duration and purposes herein;

(b) implement appropriate technical and organizational privacy measures, such as pseudonymization, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet regulatory obligations; and

(c) ensure that, by default, only Personal Data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of Personal Data collected, the extent of their processing, the period of their storage and their accessibility. The Data Controller is solely responsible for determining the business purpose and means of processing of Personal Data.

3.3 Data Processor Responsibilities. Without prejudice to the generality of clause 2.1, the Party acting as Data Processor shall, in relation to any Personal Data processed in connection with the performance by that Party of its obligations as a Data Processor herein:

(a) process Personal Data only as necessary for the performance of its obligations herein;

(b) process Personal Data only on the written instructions of the Party acting as Data Controller (unless the Party acting as Data Processor is required by the laws of any member of the EU or by the laws of the EU to process the Personal Data, in which case that Party shall promptly inform the Party acting as Data Controller of that legal requirement before processing the Personal Data, unless that law prohibits the disclosure of such information);

(c) ensure that access to the Personal Data is limited to:

(i) those members of staff who need access to the Personal Data to meet the Data Controller's obligations herein; and

(ii) in the case of access by any personnel, such part or parts of the Personal Data as is strictly necessary for performance of that member of staff's duties;

and that all personnel who have access to and/or process Personal Data are obliged to keep the Personal Data confidential;

(d) maintain complete and accurate records of any processing of Personal Data it carries out to demonstrate its compliance herein and allow for audits by the Party acting as Data Controller or its designated auditor;

(e) assist the Party acting as Data Controller, at the Data Controller's cost, in responding to any request from a Data Subject and in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;

(f) notify the Party acting as Data Controller without undue delay, and within 24 hours, on becoming aware of any Personal Data breach, such notice to include all information reasonably required by the Party acting as Data Controller to comply with its obligations under Data Protection Legislation;

(g) promptly, and in any case within five (5) business days, notify the Party acting as Data Controller 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 the Data Protection Legislation in respect of the Personal Data;

(h) ensure 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, pseudonymizing 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);

(i) employ ongoing oversight to the privacy and security obligations herein to ensure that internal controls are suitably designed and operating effectively to protect against reasonably foreseeable risks to the Data Controller's data, including, but not limited to, auditing of the privacy and security safeguards based on recognized industry best practices. Upon Data Controller's request, no more than annually, Data Processor must provide evidence that management oversight has occurred. Such evidence should briefly describe

the oversight process, indicate whether Data Processor's controls remain aligned to industry best practices, and include a signature of a corporate officer of the Data Processor.

(j) assign a qualified data protection officer when core processing activities include large scale processing of genetic, ethnic or racial personal information meeting the relevant requirements of Data Protection Law (including, where applicable, Article 37).

(k) not transfer any Personal Data across international borders unless the prior written consent of the Data Controller has been obtained and the following conditions are fulfilled:

(i) a Party has provided appropriate safeguards in relation to the transfer;
(ii) the Data Subject has enforceable rights and effective legal remedies; and
(iii) the Party acting as Data Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred.

(l) at the written direction of the Data Controller, delete or return Personal Data and copies thereof to the Data Controller on termination or expiration of the Agreement unless required by law to store the Personal Data.

3.4 Sub-Processing. The Data Controller herby provides the Data Processor general pre-authorization to use third-party data processing services so long as all obligations herein are applied to the third-party (specifically including sub-sections (a) and (b) below). The Party acting as a Data Processor will provide the Data Controller 90 days-notice before appointing a third-party processor of Personal Data herein. At such time, the Data Controller may choose to have Personal Data deleted or returned to the Data Controller. The Data Processor shall:

(a) enter with the third-party processor into a written agreement incorporating terms which offer at least the same level of protection for the Personal Data as those set out herein and which meet the requirements of Article 28 of the GDPR; and

(b) if such an arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the written agreement referred to in clause 2.4(a) above.

3.4.1 Liability for Sub-Processor. As between the Party acting as Data Controller and the Party acting as Data Processor, the Party acting as Data Processor shall remain fully liable for all acts or omissions of any third-party processor it appoints.

3.4.2 Indemnification. The Party acting as Data Processor will indemnify the Party acting as Data Controller against any loss or damage whatsoever arising from or suffered by the Party acting as Data Controller in relation to any breach by the Party acting as Data Processor of its obligations herein.

3.5 Personal Data Breach. Each Party shall use its best efforts to immediately remedy any security breach of Personal Data and prevent any further security breach at its own expense in accordance with applicable privacy rights, laws, regulations and standards.

4. Restricted Transfers.

4.1 Standard Contractual Clauses. The Parties hereby enter into the Standard Contractual Clauses with respect to any Restricted Transfer from Center (acting as Data Controller) to NMDP or to any third-party sub-processor (acting as Data Processor). The Standard Contractual Clauses shall come into effect under this clause on the later of:

(c) the Data Controller becoming a Party to them;

(d) the Data Processor becoming a Party to them; and

(e) commencement of the relevant Restricted Transfer.

4.2 Data Sharing with Associated Centers. The Parties may share data with their respective Associated Centers which request donor data required for determining the feasibility for specific transplant procedures. All such data shall be provided to the Associated Centers for this purpose only and is subject to privacy and confidentiality restrictions applicable to such data.

SCHEDULE 2

DATA PROCESSING

This Schedule 2 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 Personal Data in the provision of the Services to the other Party.

The types of the Personal Data to be Processed

Personal Data (including names, addresses, telephone numbers, email contact details, genetic, ethnic and racial information) and health information

The categories of Data Subject to whom the Personal Data relates

Donors, Patients, Biological Offspring of Patient

The obligations and rights of the Data Controller and Data Controller Affiliates

The obligations and rights of the Data Controller are set out in the Agreement and this Schedule 2.

SCHEDULE 3

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.

Name of the data exporting organisation:

Address:

Tel.: _____; fax: _____; e-mail: _____

Other information needed to identify the organisation

……

(the data **exporter**)

And

Name of the data importing organisation:

Address:

Tel.: _____; fax: _____; e-mail:_____

Other information needed to identify the organisation:

……

(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.

Background

The data exporter has entered into a data processing addendum (“DPA”) with the data importer. Pursuant to the terms of the DPA, it is contemplated that services provided by the data importer will involve the transfer of Personal Data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with Directive 95/46/EC and applicable data protection law, the controller agrees to the provision of such Services, including the processing of Personal Data incidental thereto, subject to the data importer’s execution of, and compliance with, the terms of these Clauses.

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 subprocessor 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 subprocessor 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 subprocessing 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 subprocessing, 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

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;

(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 dataexporter 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 subprocessing, 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 subprocessing, it has previously informed the data exporter and obtained its prior written consent;

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

(j) to send promptly a copy of any subprocessor 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 subprocessor 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 subprocessor 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 subprocessor 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 subprocessor 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 subprocessor agrees that the Data Subject may issue a claim against the data subprocessor 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 subprocessor 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 it 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 subprocessor, 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 subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, 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

Subprocessing

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 subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor 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 subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor 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 subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing 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 subprocessing 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 subprocessor 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 subprocessor 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.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

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

Signature……

On behalf of the data importer:

Name (written out in full):

Position:

Address:

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

Signature……

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:
[TO BE COMPLETED]

Data importer
The data importer is:
[TO BE COMPLETED]

Data Subjects
The Personal Data transferred concern the following categories of Data Subjects:
[TO BE COMPLETED]

Categories of data
The Personal Data transferred concern the following categories of data:
[TO BE COMPLETED]

Special categories of data (if appropriate)
The Personal Data transferred concern the following special categories of data:
[TO BE COMPLETED]

Processing operations
The Personal Data transferred will be subject to the following basic processing activities:
[TO BE COMPLETED]

DATA EXPORTER

Name:……

Authorised Signature ……

DATA IMPORTER

Name:……

Authorised Signature ……

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):

[TO BE COMPLETED]