## Appendix - General Data Protection Regulation

During the course of providing Services to, or on behalf of, UC pursuant to the Agreement between UC and Supplier dated ___________, Supplier may process personal data as defined below. The Parties agree that with respect to the processing of personal data pursuant to the Agreement or this Appendix – General Data Protection Regulation ("Appendix GDPR"), UC is the data controller (and shall hereinafter be referred to as the "Controller"), and Supplier is the data processor (and shall hereinafter be referred to as the "Processor"). The Parties have agreed that the Processor will provide the Services to the Controller pursuant to and in accordance with the terms and conditions of the Agreement and this Appendix GDPR. In the event of a conflict between the terms of this Appendix GDPR and the Agreement or any amendment or appendix thereto, the terms of this Appendix GDPR shall govern. Supplier agrees to be bound by the obligations set forth in this Appendix GDPR. To the extent applicable, Supplier also agrees to impose, by written contract, the terms and conditions contained in this Appendix GDPR on any third party retained by Supplier to provide Services for or on behalf of UC.

### A. Definitions

Capitalized terms used but not defined in this Appendix GDPR will have the meanings set forth in the Agreement. The following terms shall have the meanings set forth herein:

1. "**Data**" means all personal data processed by (or on behalf of) the Processor for the Controller under or in connection with the Agreement, including in the provision of the Services. If Appendix DS applies to this Agreement, "Data" as used herein shall also be considered UC Institutional Information as defined in Appendix DS.

2. "**Data Subjects' Rights**" means the rights of data subjects as provided in the GDPR including, but not limited to, rights of access, rectification, erasure, restriction of processing, data portability, objection, and the right not to be subject to automated decision making (including profiling);

3. "**EEA**" means European Economic Area;

4. "**EU**" means the European Union;

5. "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;

6. "**data subject**," "**personal data**," "**personal data breach**," "**process/processing**," "**pseudonymisation**," and "**supervisory authority**," shall each have the meaning as in the GDPR;

7. "**Subprocessor**" means any third party: (i) who is engaged by the Processor to carry out specific processing activities relating to Data for or on behalf of the Controller; or (ii) to whom the Processor subcontracts any of its obligations in connection with the Agreement.

### B. Scope of Processing Data

1. Processor shall process Data solely for the purposes of performing the Services and for the same duration of the Agreement, except as otherwise agreed to in writing by the Parties. The scope and

further details of Processor's processing activities of Data pursuant to the Agreement and Appendix GDPR are set forth in Addendum A to this Appendix GDPR.

2. To the extent any additional information is required to be included in Addendum A pursuant to the GDPR or any other applicable EU member state, or EEA state law, or this Agreement otherwise requires amendment, the Parties will cooperate to amend this Appendix GDPR in a writing signed by both Parties.

## C. Subprocessors

1. Controller generally authorizes Processor to engage Subprocessor(s) to perform any of Processor's obligations in providing Services to Controller in connection with the Agreement as set forth in Addendum A and as allowed under the terms of the Agreement, except that any processing of personal data by Subprocessor(s) outside of the United States or EEA must be specifically authorized in writing prior to such processing by Controller.

2. The Processor shall give the Controller prior written notice of any intended changes concerning the addition or replacement of any Subprocessors set forth in Addendum A to allow the Controller to approve or object to such changes. Such notice shall include details of the processing activity or activities to be conducted by the applicable Subprocessor and the identity and contact details of such Subprocessor.

3. The Processor shall ensure that any Subprocessor approved by Controller in accordance with this Section C is subject to obligations in a written agreement requiring such Subprocessor to comply with the obligations of this Appendix GDPR. If any Subprocessor fails to fulfill its data protection obligations, the Processor shall remain fully liable to the Controller for the performance or non-performance of such Subprocessor.

4. Upon request, the Processor shall provide a copy of each Subprocessor agreement entered into pursuant to this Section C to the Controller.

## D. Obligations of the Processor

1. The Processor shall, and shall ensure that each of its employees, approved Subprocessors and any other individual acting under its authority who has access to the Data:

   a. process Data in accordance with the terms of this Agreement, Appendix GDPR or any other written instructions of the Controller, and only to the extent and in the manner necessary to provide Services, and for no other purpose(s). In the event EU or member state law requires Processor to process in a manner not expressly authorized by this Agreement or the Controller's written instructions, the Processor shall promptly inform the Controller of the applicable legal requirement before processing, unless prohibited from doing so on important public interest grounds, consistent with EU or member state law;

   b. keep the Data confidential and ensure that any person authorized to process the Data for or on behalf of the Processor (including but not limited to any Processor employees and staff and approved Subprocessors) has agreed to keep the Data confidential, or is otherwise under a statutory obligation to protect the confidentiality of the Data; and

c. upon reasonable request from the Controller, provide an up-to-date copy of the Data in the format requested by the Controller.

2. In carrying out its obligations under the Agreement and this Appendix GDPR, Processor agrees to comply with all applicable state, federal and laws of other countries or jurisdictions (including, but not limited to, GDPR), as well as industry best practices, governing the collection, access, use, disclosure, safeguarding and destruction of Data.

3. In accordance with GDPR, and taking into consideration the state of the art, costs of implementation and the nature, scope, context and purposes of processing the Data pursuant to this Agreement, as well as the risks to the rights and freedoms of natural persons and the risks to processing the Data, the Processor represents and warrants that it has implemented appropriate technical and organizational security measures appropriate to such risks, including, as appropriate: (i) the pseudonymisation and encryption of the Data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability of and access to the Data in a timely manner in the event of a physical or technical incident; and (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing. Upon Controller’s request, Processor shall provide to Controller evidence demonstrating Processor’s implementation of such technical and organizational security measures as required by GDPR.

4. The Processor shall assist the Controller in ensuring compliance with Controller’s obligations as a Controller by: (a) cooperating with Controller’s implementation of appropriate technical and organizational security measures to ensure the security of processing Data; (b) cooperating with Controller notifications to supervisory authorities and/or data subjects, as applicable, of any breaches of Data; (c) cooperating with Controller’s conduct of data protection impact assessments, including but not limited to, any requirements to consult with a supervisory authority as required by GDPR. Processor shall also cooperate with additional obligations of Controller that may be required of it pursuant to GDPR and other applicable data protection laws.

5. In the event of any suspected or actual personal data breach, the Processor shall notify the Controller to the individual identified below immediately upon discovery, both orally and in writing, but in no event more than two (2) calendar days after Processor identifies or reasonably believes a personal data breach has or may have occurred. Processor’s notification to the Controller will identify: (i) the nature of the personal data breach, including where possible, the categories and the approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; (ii) a description of the likely consequences of the personal data breach; and (iii) a description of the measures taken or proposed to be taken to address the personal data breach, including where appropriate, measures to mitigate its possible adverse effects. Processor will provide such other information as reasonably requested by Controller. In the event of a suspected personal data breach, Processor will keep Controller informed regularly of the progress of its investigation until the uncertainty is resolved.

In event of suspected or actual personal data breach, the Processor shall notify:

| | | |
|---|---|---|
| **Name** | | |
| **Phone** | | |
| **Email** | | |
| **Address** | | |

6. Processor will fully cooperate with Controller's investigation of any personal data breach, including but not limited to making witnesses and documents available immediately upon Supplier's reporting of the personal data breach at no cost to Controller.

7. Any personal data breach may be grounds for immediate termination of the Agreement by Controller.

8. Except for transfers of Data to the Controller, the Processor shall not process or transfer any Data to any country outside the EEA except pursuant to prior written approval of the Controller, and at all times in compliance with GDPR and other applicable data protection laws.

9. This section is only applicable if Processor's Services include the collection of personal data directly from data subjects:

   In the event Processor's Services include the collection of personal data directly from data subjects that is to be provided to Controller, unless the parties otherwise agree, the Processor shall be responsible for ensuring that such processing of personal data complies with GDPR requirements, including, but not limited to, obtaining a lawful basis to process the personal data.

10. This section is only applicable if: (1) Processor or a Subprocessor is based in the EEA; (2) Processor's or such EEA-based Subprocessor's Services include the transfer of personal data from the EEA to Controller; and (3) data subjects have not explicitly consented to the transfer of their personal data to Controller in the United States:

    Unless the parties otherwise agree on another transfer mechanism that satisfies GDPR requirements, transfers of personal data shall be governed by the Standard Contractual Clauses set forth in Addendum B to this Appendix GDPR.

11. Processor acknowledges that Controller is subject to U.S. federal and state laws and regulations, including but not limited to public disclosure and retention laws and regulations, that may require the retention and disclosure of information that is the subject of the Agreement.

12. Within thirty (30) days of the termination, cancellation, expiration or other conclusion of this Appendix GDPR, Processor will deliver the Data to UC unless UC requests in writing that such Data be destroyed. This provision will also apply to all Data that is in the possession of Subprocessors. Such destruction will be accomplished by "purging" or "physical destruction," in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-88 Guide to Media Sanitization. Processor will certify in writing to Controller that such delivery

or destruction has been completed. In the event EU, EU member state, or EEA state law requires the storage of such Data, the Processor shall promptly inform the Controller of such requirement in writing. In such instance, Processor will continue to protect the Data in accordance with the terms of this Appendix GDPR.

## E. Data Subjects' Rights

1. Unless Section D.9 of this Agreement applies, the Controller shall be responsible for providing data subjects with any information required under GDPR at the time of collecting such data subjects' personal data, as well as any information requested by data subjects relating to the processing of their personal data.

2. The Processor shall notify the Controller (via the individual identified by UC in this Appendix GDPR) in writing (including by e-mail) of each and any request that it receives from a data subject relating to a Data Subject Right. Such written notification shall be made promptly no later than two (2) business days following receipt of the request, and shall include any information in the Processor's custody or control that may assist the Controller to respond to the request.

3. Unless otherwise required by applicable EU, EU member state, or EEA state law, the Processor shall not respond to any such requests or other communications the Processor receives from data subjects, without the prior written consent of the Controller.

4. The Processor shall assist the Controller in Controller's obligations to respond to requests for exercising Data Subjects' Rights by using appropriate technical and organizational measures, to the extent practicable given the nature of the processing of Data.

## F. Accountability

1. Upon written request from the Controller, the Processor shall make available to the Controller all information necessary to demonstrate compliance with its obligations under this Appendix GDPR. The Processor shall make its records, documents, facilities, processes and individuals reasonably available to Controller or Controller's designee for audits or inspections to demonstrate compliance with this Appendix GDPR.

2. The Processor shall immediately inform the Controller if, in the Processor's opinion, any instruction from the Controller with respect to the processing of Data pursuant to this Agreement violates or contradicts GDPR, or other applicable EU, EU member state, or EEA state data protection laws or regulations.

## Addendum A: Scope of Processing Data

This Addendum is part of the Appendix GDPR and includes details of the processing of Data as required by the Agreement.

1. Processor is processing Data on behalf of the Controller for purposes of the performance of Services described in this Agreement. Data shall be processed for the duration of the term of this Agreement, except as otherwise specifically set forth herein. [IF THE DATA WILL BE PROCESSED BY THE PROCESSOR FOR PURPOSES OF PROVIDING SERVICES BEYOND THE DURATION OF THE TERM OF THE AGREEMENT, DESCRIBE THAT HERE.]

2. The purposes(s) of the processing of Data to be carried out by the Processor on behalf of the Controller includes: [e.g., administration of payroll to employees; quality improvement of laboratory testing ]

3. The Data to be processed by the Processor on behalf of the Controller in the performance of Services includes the following: [BUYER TO IDENTIFY TYPES OF DATA, E.G., NAME, TITLE, CONTACT INFORMATION, BIRTHDATE, AGE, IDENTIFICATION NUMBERS, ACADEMIC RECORDS, FINANCIAL DATA,] [Insert, if applicable: the Data also includes the following sensitive data – [choose as appropriate]: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, data concerning sex life or sexual orientation, or data relating to criminal convictions or offenses] If the Processor becomes aware that additional personal data not identified above has been received from the Controller, the Processor shall immediately notify the Controller.

4. The Data to be processed by the Processor on behalf of the Controller in the performance of Services relates to the following categories of data subjects: [E.G., PATIENTS, STUDENTS, DONORS, EMPLOYEES, SUPPLIERS, CONSULTANTS.]

5. Controller authorizes the Processor to subcontract the following processing activities to the following Subprocessors: [insert “None” or the name and contact information of each Subprocessor, and a description of the type of processing activities the Subprocessor will conduct.]

6. Other than to the United States as may be required for the performance of Services, and for which the Controller has a lawful basis to transfer the Data to the United States pursuant to GDPR, the Processor may transfer Data to the following countries outside of the EEA: [insert “None” or information relating to the country, recipient, and details regarding how the transfer will be in compliance with GDPR. Consult OGC for guidance if the Processor requires inclusion of this Section.]

# Addendum B: Standard Contractual Clauses

**Commission Decision C(2004)5721**

**SET II**

**Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)**

Data transfer agreement

between

[SUPPLIER] ..........................................................................................................(name)

[ENTER ADDRESS]..........................................................................................(address and country of establishment)

hereinafter “data exporter”

and

The Regents of the University of California, on behalf of its ________ location....(name)

[ENTER ADDRESS]..........................................................................................(address and country of establishment)

hereinafter “data importer”

each a “party”; together “the parties”.

**Definitions**

For the purposes of the clauses:

a) “personal data”, “special categories of data/sensitive data”, “process/processing”, “controller”, “processor”, “data subject” and “supervisory authority/authority” shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby “the authority” shall mean the competent data protection authority in the territory in which the data exporter is established);

b) “the data exporter” shall mean the controller who transfers the personal data;

c) “the data importer” shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country’s system ensuring adequate protection;

d) “clauses” shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

## I. Obligations of the data exporter

The data exporter warrants and undertakes that:

a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.

b) It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.

c) It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.

d) It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.

e) It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

## II. Obligations of the data importer

The data importer warrants and undertakes that:

a) It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

b) It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.

c) It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.

d) It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.

e) It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).

f) At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).

g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.

h) It will process the personal data, at its option, in accordance with:

i. the data protection laws of the country in which the data exporter is established, or

ii. the relevant provisions of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is based in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data, or

iii. the data processing principles set forth in Annex A.

Data importer to indicate which option it selects: Annex A ...............................................................

Initials of data importer: [COMPLETE] ............................................................................................;

i) It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and

i. the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or

ii. the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or

iii. data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or

iv. with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer

## III. Liability and third party rights

a) Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.

b) The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

## IV. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

## V. Resolution of disputes with data subjects or the authority

a) In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

b) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

c) Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

## VI. Termination

a) In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

b) In the event that:

i. the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);

ii. compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;

iii. the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;

iv. a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or

v. a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs

then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

c) Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

## VII. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

## VIII. Description of the Transfer

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

Dated:...........................................................

[FOR DATA IMPORTER

....................................................................

....................................................................]

[FOR DATA EXPORTER

..............................................................................

...............................................................................]

ANNEX A

## DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.

2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.

4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.

5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.

6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.

7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to “opt-out” from having his data used for such purposes.

8. Automated decisions: For purposes hereof “automated decision” shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:

   a) i. such decisions are made by the data importer in entering into or performing a contract with the data subject, and

   ii. the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.

   or

   b) where otherwise provided by the law of the data exporter.

## ANNEX B

## DESCRIPTION OF THE TRANSFER

(To be completed by the parties)

**Data subjects**
The personal data transferred concern the following categories of data subjects:
See Addendum A: Scope of Processing Data, Section 4.

**Purposes of the transfer(s)**
The transfer is made for the following purposes:
See Addendum A: Scope of Processing Data, Sections 1 and 2.

**Categories of data**
The personal data transferred concern the following categories of data:
See Addendum A: Scope of Processing Data, Section 3.

**Recipients**
The personal data transferred may be disclosed only to the following recipients or categories of recipients:
See Addendum A: Scope of Processing Data, Section 5. If applicable, Data importer may also transfer to the data to the following types of recipients:[TO BE COMPLETED BY BUYER]
…………………………………………………………………………………………………………………
…………………………………………………………………………………………………………………
…………………………………………………………………………………………………………………
………………………………………………………………………………………

**Sensitive data** (if appropriate)
The personal data transferred concern the following categories of sensitive data:
See Addendum A: Scope of Processing Data, Section 3. …

**Data protection registration information of data exporter** (where applicable)
[TO BE COMPLETED BY SUPPLIER]
…………………………………………………………………………………………………………………
…………………………………………………………………………………………………………………
…………………………………………………………………………………………………………………
……………………………………………………………………………………………

**Additional useful information** (storage limits and other relevant information)
The data will be protected as set forth in the Agreement. [ADD ADDITIONAL TERMS AS REQUESTED BY SUPPLIER.]
…………………………………………………………………………………………………………………
…………………………………………………………………………………………………………………
…………………………………………………………………………………………………………………
……………………………………………………………………………………………

**Contact points for data protection enquiries**

**Data importer**
[ADD PRIVACY OFFICER CONTACT]
………………………………………………
………………………………………………
………………………………………………

**Data exporter**
[TO BE COMPLETED BY SUPPLIER]
…………………………………………………
…………………………………………………
…………………………………………………