1. **Grant of Rights to Access and Conditions of Use.**

A. AgilityHealth (the Licensor) hereby grants to Licensee a limited, revocable, nonexclusive, nontransferable, non-sublicensable right and license to access, use, execute and display the Software on its internal computer screens and to generate outputs from the Software as designed and intended per descriptions in the Software's relevant documentation. Where applicable, potential or actual agents and contractors for Licensee may also access and use the Software provided they do so solely for Licensee's benefit and internal business purposes.

B. Licensor will not be liable or held at fault for any performance or operational problems resulting from Licensee's or Licensee's employees' or contractors' non-conformance to the published guidelines and technical specifications necessary for access to the Software. Also, Licensor shall not be liable or held to be in default of performance or operational obligations due to any technical or design problem within the Licensee's electronic network that compromises its employees' access to the Software or cloud servers.

C. Licensee's use of the Software shall be limited to Licensee's regular internal business matters. Neither the Software, nor the hard-copy outputs generated from Licensee's use of the Software (including use by Licensee's employees and Licensee's contractors), may be used by or disclosed to any parties outside the Parties to this Agreement without the Licensor's prior written consent, except as may be required in connection with inquiries by government or regulatory authorities, and shall always contain Licensor's copyright notice. In the event that Licensee receives any request or demand to produce or disclose any portion of the Software or outputs from the Software for any reason, to any party, including any attorney, court or government or regulatory authority, Licensee shall first promptly contact Licensor in order to provide Licensor notice of such request or demand so that Licensor may pursue its rights to object to, limit or prevent such disclosure.

D. Licensee must take appropriate measures to adequately protect Licensor's proprietary materials to prevent unauthorized parties to have access to Licensor's proprietary materials. Licensee must notify its contractors in writing that access to Licensor's Software does not grant them any ownership interest or license to Licensor's proprietary materials. In addition, Licensee shall require that any such contractors allowed access to the Software, shall implement and maintain practices and policies sufficient to preserve the confidentiality of all Licensor's proprietary materials covered under this Agreement, and Licensee shall be responsible for any breach of confidentiality, misappropriation, and/or infringement with respect to Licensor's proprietary materials. Licensee shall not transfer or sublicense the Software to any third party, in whole or in part, in any form, whether modified or unmodified.

E. This Agreement does not create a partnership or joint venture between the Parties, and does not make either Party the employee, agent or legal representative of the other for any purpose whatsoever. Neither Party is granted any right or authority to assume or create any obligation or responsibility, express or implied, on behalf of or in the name of the other Party.

2. **AgilityHealth® Assessment Data and Results.**

A. Licensor shall deliver to Licensee participant data generated from Licensee's authorized use of the Software. Notwithstanding the foregoing, Licensor reserves the right to use the foregoing information and the content of any usage statistics, results, and reports generated from Licensee's use of the Software in aggregated form for the purposes of statistical norming and research and development. Licensor also reserves the right to edit verbatims and recorded interviews (if and when applicable) to remove content that might identify a respondent or their organization.

B. Certain services that Licensor provides require that Licensor protect the anonymity of the participants in order to protect the integrity and value of the services and to protect the individual participants. In these limited circumstances, notwithstanding the terms of Section 3.A. above, Licensee will not own or have access to the line item responses provided at the participant level.

C. For compliance with the EU General Data Protection Regulation (the "GDPR"), the Parties shall comply with the provisions of this Agreement.

3. **Protection of Software Being Accessed.**

A. The Software is the exclusive property or licensed intellectual property of Licensor, and Licensor (on behalf of itself and its licensors) retains all rights to the application, manufacture, development, use, display, reproduction, modification and transfer of the Software and all rights to all worldwide patents and copyrights for the Software, including any derivative works thereof. Licensee recognizes that Licensor regards the Software as its proprietary materials and as confidential trade secrets of significant value.

B. Licensee further agrees to treat the Software with at least the same degree of care with which Licensee treats its own Confidential Information (as defined below), and in no event with less care than is reasonably required to protect the confidentiality of the Software. Licensee shall at all times exercise all due and diligent precautions to protect the integrity of Licensor's Confidential Information. Licensee's limited, restricted use license to the Software does not include the right to disclose Licensor's intellectual property to third parties without Licensor's consent.

(i) Licensee shall promptly notify Licensor in writing of any unauthorized use, infringement, misappropriation, dilution or other violation of Licensor's proprietary materials provided to Licensee of which it becomes aware.

(ii) Licensee acknowledges and understands that in the event of any breach of this Section of the Agreement, Licensor shall be entitled to specific performance and injunctive relief as remedies for any such breach. Such remedies shall not be deemed to be the exclusive remedies for a breach of this Section of the Agreement, but shall be in addition to all other remedies available to Licensor at law or in equity. If Licensor brings an action to enforce any provision of this Agreement, Licensor, if the prevailing party, shall be entitled to reasonable attorneys' fees and court costs.

C. ANY WARRANTIES ARISING IN THE COURSE OF DEALING, USAGE OR TRADE PRACTICE ARE EXCLUDED AND EXCEPT AS OTHERWISE PROVIDED IN THE TERMS OF THIS AGREEMENT, LICENSOR DISCLAIMS ALL OTHER WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE. LICENSEE IS RESPONSIBLE FOR LICENSEE'S SELECTION AND USE OF THE SOFTWARE AND SERVICES PROVIDED BY LICENSOR.

4. **Exclusions.**

Except as expressly authorized herein, Licensee and its agents, employees or consultants shall not: (i) copy the Software, or any content contained in the Software, in whole or in part - this specifically prohibits Licensee from copying the Software, including any text of content contained therein such as competencies, assessment questions, radar design, dimensions and categories, or videos - into any other system, format, media or software product, without Licensor's prior written consent; (ii) reverse compile, reverse assemble, or access with intent to "hack" all or any portion of the Software; (iii) distribute, market, rent, lease, sublicense, provide access to, or transfer the Software to third parties; (iv) modify the Software except as otherwise provided in this Agreement; or (v) remove or alter any trademark, logo, copyright or other proprietary notices, legends, symbols or labels in or on the Software. No license, right, or interest in any of Licensor's trademarks, trade names, or service marks is granted hereunder. The provisions set forth in this Section 5 shall survive termination or expiration of this Agreement.

5. **Confidential Information.**

"**Confidential Information**" means any non-public information of the Parties hereto relating to its business activities, operations, financial affairs, technology, marketing or sales plans that is disclosed to, and received by, the other Party pursuant to this Agreement. The Software includes Confidential Information which are Licensor's trade secrets, including the design, form and function of all information screens, input screens and output screens. Licensee shall utilize its best efforts to prevent disclosure of such information, at least to the extent that it protects its own Confidential Information.

6. **Governing Law/Venue**.

This Agreement shall be governed and interpreted by the laws of the State of Nebraska, USA. The appropriate venue and jurisdiction for the resolution of any disputes hereunder will be in Douglas County, Nebraska, USA.

7. **Assignment**.

Neither Party may assign this Agreement, or any of its rights under this Agreement, without the other Party's prior written consent; notwithstanding the foregoing, Licensor may assign this Agreement, upon written notice but without consent, to a successor-in-interest to substantially all of the business or in the event of internal business restructuring of Licensor. Any assignment attempted in violation of this Agreement will be null and void.

8. **Entire Agreement**.

This Agreement sets forth the entire understanding between the Parties with respect to the subject matter hereof, and merges and supersedes all prior agreements, discussions and understandings, express or implied, concerning such matters.

Data Privacy and Security Addendum

This Data Privacy and Security Addendum ("Addendum") is made a part of the attached Agreement between Agile Transformation, Inc. d/b/a AgilityHealth ("Licensor") and Licensee. In the event of a conflict or inconsistency between the terms and conditions of the Agreement and this Addendum, the terms and conditions of this Addendum shall prevail except as otherwise specifically set forth in this Addendum. Capitalized terms used and not defined in this Addendum shall have the meanings given in the Agreement.

To the extent Licensor processes personal data of individuals within the European Union, European Economic Area and Switzerland ("EU") in connection with its performance of the Agreement, "DP Law" shall be deemed to include: (i) EU Regulation 2016/679 ("GDPR"), (ii) the Swiss Data Protection Act ("DPA"), and any equivalent, replacement or similar legislation implemented in the United Kingdom after that date, whether in light of the United Kingdom's withdrawal from the European Union or otherwise.

1. **Definitions**. For purposes of this Addendum, the following terms have the meanings prescribed in this Section, irrespective of capitalization.

A. **Data Subject** means a natural person that can be identified by any Personal Data.

B. **Licensee Data** means any Personal Data or Pseudonymized Data.

C. **Personal Data** means any information that (i) Licensor possesses or is able to access arising out of its performance under the Agreement; and (ii) can be used to directly or indirectly identify a natural person.

D. **Processing** means any operation or set of operations that (i) arises out of Licensor's performance under this Agreement; and (ii) is performed upon Personal Data.

E. **Pseudonymized Data** means Personal Data which has been transformed into a form which is not attributable to a specific Data Subject without the use of additional information.

F. **Restricted Transfer** means one of the following transfers, but only where such transfer would be prohibited by DP Law (or by the terms of data transfer agreements put in place to address the data transfer restrictions of DP Law) in the absence of the Standard Contractual Clauses to be established under Section 9 below:

(i) a transfer of personal data from Licensee to Licensor; or

(ii) an onward transfer of personal data from Licensor to a processor on behalf of Licensee.

G. **Standard Contractual Clauses** means the Clauses in Addendum C, as they may be amended from time to time in accordance with Section 12.

2. **Processing**. Irrespective of Licensor's role as a "controller," Licensor shall process Licensee data only for the benefit of Licensee, and not for its own or a third party's benefit. Notwithstanding the foregoing, Licensor may use pseudonymized data for its own benefit as permitted under the Agreement. Licensor shall keep any additional information which could be combined with any pseudonymized data to identify a data subject separate from all pseudonymized data, and implement technical and organizational measures designed to prevent such identification.

3. **Administration**. Licensor shall implement and maintain appropriate technical and organizational measures (e.g., encryption of personal data, access control, logs, audits, instructions, trainings, ability to restore the availability and access to personal data in a timely manner, etc.) designed to reasonably safeguard all personal data against unintentional or illegal destruction or unintentional loss, modification, unauthorized disclosure, or unauthorized access in view of the risks associated with the processing and type of the data to be protected. At a minimum, these technical and organizational measures shall comply with the requirements set forth in Art. 32 GDPR and any applicable DP Law.

4. **Contractors**. Licensor shall ensure that only authorized persons have access to, and otherwise process, Licensee Data, and that such persons have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and shall comply with the provisions of this Addendum as applicable to them. This shall also apply to any affiliate, subcontractor, supplier and other party on the part of Licensor that are given access to or otherwise process personal data by or for Licensor. Upon request, Licensor shall disclose the names, address, contact details and function of any such parties. To the extent that such parties are processors for Licensor under GDPR with respect to personal data under DP Law, they shall be bound pursuant to Art. 28 GDPR or the equivalent provision of applicable DP Law. Licensor shall be responsible for such parties and any other persons on its part with access to Licensee Data as it is for itself under this Agreement or any DP Law. Any personal data shall be considered Confidential Information of Licensee under this Agreement.

5. **Licensee Disclosure; Licensor Return**. Licensee shall ensure that it is permitted under DP Law to disclose Licensee Data to Licensor as per this Addendum, and that data subjects have been informed as to the processing of their personal data by Licensee in compliance with DP Law. Licensor shall at any time upon request return to Licensee any personal data processed by it, with or without (as per Licensee's request) keeping a copy of it except as required by applicable law. Licensee shall supply all personal data to Licensor in a format compatible with Art. 20 GDPR.

6. **Data Subject Requests**. The responsibility for, and the control over, handling data subject requests in connection with Licensee Data shall be with Licensee, unless a data subject request expressly indicates that it is to be handled by Licensor and not by Licensee. Licensor shall without delay forward to Licensee any such request. Licensor shall assist Licensee with Licensee's technical and organizational measures required to fulfill such requests insofar as Licensor is required to do so under DP Law, taking into account the nature of Licensor's processing and of the Licensee data.

7. **Infringement of GDPR**. Each Party shall inform the other Party immediately if it has reason to believe that the processing of Licensee Data under or in connection with this Agreement infringes any DP Law or this Addendum or if it has reason to believe that it can no longer comply with this Addendum, including any request by a supervisory authority concerning Licensee Data or the processing of such Licensee Data (except where applicable law prohibits such information), if such information could be of relevance for the other Party in its capacity as a data controller; the Parties shall cooperate in responding to requests of supervisory authorities. Licensor shall not make any filing, notification or other registration with a public authority or other party that contains personal data or otherwise discloses the identity of Licensee without the express written approval of Licensee, unless prohibited by applicable law, in which case Licensor shall inform Licensee as soon thereafter as is reasonably possible.

8. **Notice**. Licensor shall notify Licensee without undue delay after becoming aware of any actual security breach pertaining to personal data as required by DP Law and provide the information, as per Article 33 para. 3 GDPR and corresponding provisions of other applicable DP Law, available to Licensor regarding: (a) the nature of the personal data breach, including, if possible, the categories and the

approximate number of affected data subjects and the categories and the approximate number of affected personal data records; (b) probable consequences of a personal data breach; and (c) measures which have been taken or are proposed to manage the personal data breach, including, if applicable, measures to limit its possible damage. This shall apply even if Licensor concludes that Licensee itself has no data breach notification obligation in the specific case. The reporting of a data breach to the authorities shall be undertaken by each Party on its own, with prior consultation of the other Party and subject to the foregoing paragraph; any notifications to the data subjects shall be done through, and by, Licensee.

9. **Access; Transfer**. Licensor shall not permit any access to personal data from outside the European Economic Area, except with the written approval of Licensee or where such access occurs by Licensee or parties acting on behalf of Licensee. In light of the foregoing, the Parties acknowledge and agree approval shall be granted for having Licensee data stored by Microsoft in its European Azure Cloud. To the extent that the transfer of personal data out of the European Union is required, the Parties agree that such transfer shall be made in compliance with this Section 9.

   A. Subject to the other subsections of this Section 9, Licensee (as "data exporter") and Licensor (as "data importer") hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfer from that Licensee to Licensor.

   B. The Standard Contractual Clauses shall come into effect under Section A only after all three of the following events have occurred:

      (i) the data exporter becomes a party to them;

      (ii) the data importer becomes a party to them; and

      (iii) the relevant Restricted Transfer commences.

   C. Section A shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from data subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable DP Law.

   D. If either Party determines in its reasonable discretion that Restricted Transfers will no longer be required under this Agreement after the Standard Contractual Clauses have come into effect under Section 9.B., that Party may deliver notice of its determination to the other Party.

      (i) If the other Party consents or does not respond to the notice of such determination within thirty (30) days after such notice was delivered, the Standard Contractual Clauses shall be deemed inactive under this Agreement.

      (ii) If the other Party objects to the first Party's determination, then the Standard Contractual Clauses shall remain in effect.

   E. If the Standard Contractual Clauses are inactive pursuant to Section 9.D.(i), they may be revived at a later date by any of the triggering events under Section 9.B.

   F. Any notice or objection made pursuant to Section 9.D. shall not affect either Party's rights under Section 12.

10. **Audit**. Licensor shall make available to Licensee all information and access necessary to demonstrate

and verify Licensor's compliance with this Addendum and DP Law in processing Licensee personal data and allow for and contribute to audits, including inspections, conducted by the Licensee or another auditor mandated by Licensee to achieve the foregoing.

11. **Costs**. Each Party shall bear its own costs for implementing this Addendum, and compliance with DP Law, except that each Party shall indemnify and hold the other Party harmless against any liability, claims, losses, costs and expenses arising from the indemnifying Party's violations of this Addendum or any DP Law.

12. **Changes in DP Law**.

    A. Either Party may:

        (i) by at least thirty (30) days' written notice to the other Party, from time to time make any variations to the Standard Contractual Clauses (including any Standard Contractual Clauses entered into under Section 9), as they apply to Restricted Transfers which are subject to a particular DP Law, if such changes are required as a result of any change in or decision of a competent authority under the applicable DP Law, in order to allow those Restricted Transfers to be made (or continue to be made) without breach of that DP Law; and

        (ii) propose any other variations to this Addendum which either Party reasonably considers to be necessary to address the requirements of any DP Law.

    B. If either Party gives notice under Section 12.A.(i) or proposes other variations under Section 12.A.(ii), the other Party shall not unreasonably withhold or delay its agreement to any variations to this Addendum reasonably designed to mitigate the risks identified in such notice.

    C. If either Party gives notice under Section 12.A.(ii), the Parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in such Party's notice as soon as is reasonably practicable.

13. **Severability**. Should any provision of this Addendum be determined by a court of competent jurisdiction to be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either:

    A. amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible;

    B. construed in a manner as if the invalid or unenforceable part had never been contained therein.

Standard Contractual Clauses Addendum

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

Definitions

For the purposes of the clauses of and the Annexes to this Addendum:

(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.

(e) "Agreement" means the Agreement to which this Addendum is attached.

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 organizational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized 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 authorizes 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 authorized 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 organization authorized 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[1] 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 authorization or decision and is based in a country to which such an authorization or decision pertains, but is not covered by such authorization or decision for the purposes of the transfer(s) of the personal data[2], or

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

(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

[1] "Relevant provisions" means those provisions of any authorization or decision except for the enforcement provisions of any authorization or decision (which shall be governed by these clauses).
[2] However, the provisions of Annex A.5 concerning rights of access, rectification, deletion and objection must be applied when this option is chosen and take precedence over any comparable provisions of the Commission decision selected.

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.

ANNEX A to STANDARD CONTRACTUAL CLAUSES ADDENDUM

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 authorized 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 organizational 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, unauthorized 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 organization 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 organizations 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 organization 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.