Data Protection Addendum

1. Purpose

This Data Protection Addendum ("Addendum") supplements the terms and conditions in the Agreement as they relate to WellRight's Processing of Personal Data and compliance with Data Protection Law. Notwithstanding anything to the contrary in the Agreement, if there is a conflict between this Addendum and the Agreement, this Addendum will control. The terms of this Addendum shall only apply to the extent WellRight receives Personal Data that is subject to Data Protection Law.

2. Definitions

Capitalized terms used but not defined have the meaning given in the Agreement. Other terms in this Addendum, which are not defined in the Agreement or this Addendum, shall have meanings consistent with any corresponding terms in Data Protection Law.

a) "Data Protection Law" means any Applicable Law, relating to data security, data protection and/or privacy, including 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 processing of personal data and the free movement of that data ("GDPR") and the California Consumer Privacy Act (Cal. Civ. Code § 1798.100 et. seq.) ("CCPA"), and any implementing, derivative or related legislation, rule, regulation, and regulatory guidance, as amended, extended, repealed and replaced, or re-enacted.

b) "Personal Data" means any information relating to, describes, is reasonably capable of being associated with, or could reasonably be linked to an identified or identifiable natural person ("Data Subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by referencing an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

c) "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, whether transmitted, stored, or otherwise Processed.

d) "Privacy Shield" means the Swiss-U.S. Privacy Shield or the EU-U.S. Privacy Shield and any successor framework, in each case, to the extent recognized as providing adequate data protection under Data Protection Law.

e) "Processing" means any operation or set of operations that is performed on Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction. "Process" and "Processed" will have a corresponding meaning.

f) "Standard Contractual Clauses" means the standard contractual clauses and related appendices, attached as Schedule 3 to this Addendum, in the form mandated by and pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries or in the form mandated by and pursuant to another European Commission decision authorizing the use of standard contractual clauses to safeguard a transfer to processors or sub-processors in accordance with Data Protection Law.

3. GDPR Requirements

a) Without limiting WellRight's obligation to comply with the GDPR, WellRight, in its capacity as a data processor or sub-processor of Personal Data on Client's behalf, will:

(i) Process Personal Data only on documented instructions from Client, including with regard to transfers of Personal Data to a third country or an international organization, unless required to do so by European Union or Member State law to which WellRight is subject. In such case, WellRight will inform Client of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest;

(ii) Ensure that persons authorized to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(iii) Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the Processing, including all measures required pursuant to Article 32 of the GDPR;

(iv) Taking into account the nature of the Processing, assist Client by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Client's obligation to respond to requests for exercising the Data Subject's rights laid down in Data Protection Law (including Chapter III of the GDPR);

(v) Reasonably assist Client with its obligations relating to data security, Personal Data Breach, data protection impact assessments, and engaging in legally required consultations with a competent supervisory authority, pursuant to Data Protection Law (including Articles 32 to 36 of the GDPR taking into account the nature of processing and the information available to WellRight);

(vi) At the choice of Client, promptly delete or return all the Personal Data to Client after the end of the provision of Services relating to Processing, and delete existing copies unless European Union or Member State law requires storage of Personal Data;

(vii) Without limiting any of Client's existing audit rights under the Agreement (if any), make available to Client all information reasonably necessary to demonstrate compliance with Data Protection Law (including the obligations laid down in Article 28 of the GDPR) and allow for and contribute to reasonably frequent audits, including inspections, conducted by Client or another auditor mandated by Client, provided that (i) each party shall bear its own costs in connection with an audit up to one (1) audit per contractual year and (ii) for any further audits during the same contractual year, Client shall bear the costs and (iii) each party shall always bear its own costs in relation to audits initiated by a competent supervisory authority; and

(viii) Immediately inform Client if, in its opinion, an instruction infringes Data Protection Law.

b) Client agrees that WellRight may engage third party sub-processors to process Personal Data in accordance with this Section.

(i) Client hereby authorizes WellRight to appoint the sub-processors specified in Schedule 2 of this Addendum.

(ii) WellRight shall provide Client prior notice of any additional or replacement sub-processors. After being notified, Client must notify WellRight within ten (10) business days of any reasonable objection it has to such sub-processors. Failure to notify WellRight within this time frame will constitute approval of such sub-processors.

(iii) In the event Client provides reasonable objection pursuant to Section 3(b)(ii), WellRight will use commercially reasonable efforts to make a change in Processing under the Agreement to avoid Processing of Personal Data by such sub-processor. If WellRight is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, Client may terminate services provided under the Agreement in respect only to those services which cannot be provided by WellRight without the use of the objected-to sub-processor, by providing written notice to WellRight. Client shall receive a refund of any prepaid fees for the period following the effective date of termination in respect of such terminated services.

(iv) In the event WellRight engages sub-processors under the Agreement, WellRight shall place the same or similar obligations in all material respects as those in this Addendum on such sub-processors or other obligations required by Data Protection Law. WellRight shall remain fully liable to Client for such sub-processors' performance of their obligations arising out of the Agreement.

c) WellRight will notify Client without undue delay upon becoming aware of a Personal Data Breach.

d) Where Client faces an actual or potential claim arising out of or related to violation of any Data Protection Law (e.g., Article 82 of the GDPR) concerning the Services, WellRight will promptly provide all materials and information reasonably requested by Client that are available to WellRight and relevant to the defense of such claim and the underlying circumstances concerning the claim.

e) The subject matter of the Processing is described in Schedule 1 of this Addendum. Client's instructions relating to the Processing will be documented in the Agreement or another written agreement signed by the parties' authorized representatives.

f) WellRight will comply with Data Protection Law.

4. CCPA Requirements

a) WellRight shall not retain, use, or disclose Personal Data for any purpose other than to perform the services under the Agreement or otherwise as permitted by the CCPA, including retaining, using, or disclosing the Personal Data for a commercial purpose other than providing such services.

b) Upon the direction of Client in response to a Verifiable Consumer Request (as defined by the CCPA) to delete Personal Data, WellRight shall delete Personal Data within the scope of the request unless the CCPA authorizes further retention by WellRight.

c) WellRight shall Process Personal Data in accordance with applicable CCPA requirements.

5. Legal Requests for Personal Data

Unless prohibited by applicable law, in the event that WellRight is required by law, court order, warrant, subpoena, or other legal judicial process ("**Legal Request**") to disclose any Personal Data to any person or entity other than Client, WellRight shall notify Client promptly and shall provide all reasonable assistance to Client, at Client's cost, to enable Client to respond or object to, or challenge, any such demands,

requests, inquiries or complaints and to meet applicable statutory or regulatory deadlines. WellRight shall not disclose Personal Data pursuant to a Legal Request unless it is required to do so and has otherwise complied with the obligations in this Section.

6. International Transfers of Personal Data

Where Personal Data originating in the European Economic Area, United Kingdom, or Switzerland is Processed by WellRight outside the European Economic Area, United Kingdom, or Switzerland in a territory (including a legal framework, such as the Privacy Shield) that has not been designated by the European Commission, United Kingdom or Switzerland as ensuring an adequate level of protection pursuant to Data Protection Law, WellRight and Client agree that any transfer or onward transfer shall be undertaken pursuant to Standard Contractual Clauses. The Standard Contractual Clauses apply to Client or the affiliates of Client established within the European Economic Area, Switzerland or the United Kingdom that have signed Order Forms or are otherwise entitled to receive Services under the Agreement. For the purpose of the Standard Contractual Clauses, Client or the affiliates of Client shall be deemed "data exporters." For transfers from Switzerland only, the term "personal data" as used in the Standard Contractual Clauses, shall have the meaning give under the Swiss Data Protection Act, as amended or replaced from time to time.

Effective Date: August 17, 2020

Appendix 1 to Addendum – Details of Processing

Nature and Purpose of Processing

Processing of Personal Data as necessary for WellRight to provide the Service as defined by and in accordance with the Agreement.

Categories of Data Subjects

Client may submit or otherwise provide access to Personal Data through the use of the Service, the extent of which is determined and controlled by Client in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Employees and contractors of Client
- Authorized end users of the Service

Categories of Personal Data

Client may submit or make available Personal Data to the Services, the extent of which is determined and controlled by Client in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Localization and demographic data
- Contact information (email, phone, physical address, mailing address)
- Data concerning health
- ID data
- IP address and device and browser data
- Data relating to usage of the Service

Duration of Processing

Subject to Section 3(a)(vi) of the Addendum, WellRight stores Personal Data for term of the Agreement and 90 days thereafter.

Schedule 2 to Addendum – Sub-Processors

The sub-processors listed below have been engaged to by WellRight on or before the Effective Date, and may assist in Processing within the scope of Service provided to Client under the Agreement.

Sub-Processor Name	Description of Sub-Processors' Activities
Amazon Web Services (AWS)	Provides hosting services for the web infrastructure and databases
Validic	Mobile health API connection to access user data gathered from clinical devices, and wearables devices
eHealthScreenings	Provides biometric screening services
Tango Card	E-Gift Card Rewards and Incentives management services
Marquee Health	Provides employers with an outcomes-driven suite of health and wellness programs
Twilio	Provides transactional SMS services

Schedule 3 to Addendum – Standard Contractual Clauses

STANDARD CONTRACTUAL CLAUSES

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

Client,

as defined in the Agreement and as further specified in the Addendum

(the **data exporter**)

And

WellRight, Inc.

175 W Jackson Blvd, Suite 1425, Chicago, IL 60604

(the **data importer**)

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

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 ("Addendum") with the data importer. Pursuant to the terms of the Addendum, 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 6.2, Clause 7, Clause 8.2, and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8.2, and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-Processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8.2, and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent,

unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor 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:

1. 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;

2. 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;

3. that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2;

4. 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;

5. that it will ensure compliance with the security measures;

6. 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;

7. to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8.3 to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

8. to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses,

unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

9. that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor 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

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

Clause 5

OBLIGATIONS OF THE DATA IMPORTER

The data importer agrees and warrants:

1. 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;

2. 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;

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

4. that it will promptly notify the data exporter about:

    a. 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,
    b. any accidental or unauthorised access, and
    c. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

5. 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;

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

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

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

9. that the processing services by the sub-processor will be carried out in accordance with Clause 11;

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

Clause 6

LIABILITY

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

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 6.1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 6.1 and 6.2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-Processor shall be limited to its own processing operations under the Clauses.

Clause 7

MEDIATION AND JURISDICTION

1. The data importer agrees that if the data subject invokes against 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 sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 8.2. 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 Clauses.

Clause 11

SUB-PROCESSING

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

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in Clause 6.1 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 11.1 shall be governed by the law of the Member State in which the data exporter is established.

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

Clause 12

OBLIGATION AFTER THE TERMINATION OF PERSONAL DATA PROCESSING SERVICES

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

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 7.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

DESCRIPTION OF THE TRANSFERS (CONTROLLER TO PROCESSOR)

This Appendix forms part of these Clauses.

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:

Client or affiliates of Client as described in Section 6 of the Addendum.

Data importer

The Data Importer is:

WellRight, Inc., 175 W Jackson Blvd, Suite 1425, Chicago, IL 60604

Data subjects

The personal data transferred concern the following categories of data subjects:

Data exporter may submit or otherwise provide access to Personal Data through the use of the Service, the extent of which is determined and controlled by data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Employees and contractors of data exporter
- Authorized end users of the Service

Categories of data

The personal data transferred concern the following categories of data:

Data exporter may submit or make available Personal Data to the Services, the extent of which is determined and controlled by data exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Localization and demographic data
- Contact information (email, phone, physical address, mailing address)
- ID data
- IP address and device and browser data
- Data relating to usage of the Service

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data:

Health information

Processing operations

The personal data transferred will be subject to the following basic processing activities:

Use of personal data for the provision of the Services as described in an applicable Order Form and the purpose of communications between the parties.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

This Appendix 2 forms part of the Clauses.

Data importer will maintain appropriate technical and organizational security measures to protect the Personal Data against accidental or unlawful destruction or accidental loss, damage, alteration, unauthorized disclosure or access in accordance with the Addendum and requirements under Data Protection Law.