Data Processing Addendum

This Data Processing Addendum ("**DPA**") supplements the Agreement between Humanity and Customer (jointly "the Parties"), when the General Data Protection Regulation ("**GDPR**") applies to your use of Humanity's Services to Process Customer Data. Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between any other agreement between the Parties including the Agreement and this DPA, the terms of this DPA will control.
This DPA was last updated August 1, 2020. Humanity reserves the right to periodically update and modify this DPA upon written notice to Customer, and such modification will automatically become effective in the next service term. Archived versions of this DPA are available here.

1. Definitions. Unless otherwise defined in the Agreement, all capitalized terms used in this DPA will have the meanings given to them below.

1.1 "Agreement" means any agreement between Humanity and a specific customer under which Services are provided by Humanity to that customer. Such an agreement may have various titles, including but not limited to "Order Form," "Sales Order," or "Terms of Service."
1.2 "Customer" means the entity which determines the purposes and means of Processing of Customer Data.
1.3 "Customer Data" means any "personal data" (as defined in GDPR) that is provided by or on behalf of Customer and Processed by Humanity pursuant to the Agreement.
1.4 "Data Protection Laws" means all laws and regulations, including laws and binding regulations of the European Union, the European Economic Area ("EEA") and their member states, Switzerland and the United Kingdom, and any amending or replacement legislation from time to time, applicable to the Processing of Customer Data under the Agreement.
1.5 "GDPR" means the General Data Protection Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the Processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC.
1.6 "Permitted Purpose" means the use of the Customer Data to the extent necessary for provision of the Services by Humanity to the Customer.
1.7 "Security Incident" means any unauthorized or unlawful access to, or acquisition, alteration, use, disclosure, or destruction of Customer Data.
1.8 "Services" means the Humanity services that are ordered by the Customer from Humanity.
1.9 "Standard Contractual Clauses" means the agreement, attached at Annex 2, pursuant to the European Commission decision (C(2010)593) of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC.
1.10 "Sub-processor" means any entity engaged by Humanity to Process Customer Data in connection with the Services.
1.11 "Supervisory Authority" means an independent public authority which is established by an EU Member State pursuant to the GDPR.
1.12 Terms such as "Data Subject," "Processing," "Controller," and "Processor" shall have the meaning ascribed to them in the GDPR.
1.13 "Third-Party Services" means connections and/or links to third party websites and/or services not included in the core Services offerings identified in the Agreement, including, without limitation, via application programming interfaces.

2. Data Processing

2.1 <u>Details of Processing</u>.
2.1.1 Subject Matter. Humanity's provision of the Services to the Customer.
2.1.2 Nature and Purpose. Humanity will process Customer Data for the purposes of providing the Services (including administration, operations, technical and customer support), to Customer in accordance with the Terms.
2.1.3 Data Subjects. Data Subjects include the individuals about whom data is provided to Humanity via the Services by or at the direction of the Customer. These include:
2.1.3.1 Natural persons who submit personal data to Customer via use of the Services (including employee information and email communication hosted by Humanity on behalf of Customer) ("Applicants").
2.1.3.2 Natural persons who are employees, representatives, or other business contacts of the Customer.
2.1.4 Categories of Data. Data relating to individuals provided to Humanity via the Services, by or at the direction of Customer. The Customer may submit Customer Data to the Services, and may request for its Employees to submit Employee Data to the Services, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, without limitation:
2.1.4.1 Customer Data of all types that may be submitted by Employees of the Customer via the Services for the purpose of workforce management information that enables the employee to access work schedule information. For example: name, geographic location, employment start date, contact details, position, location, gender, skills, certifications, wages and other preferences and other personal details that the data exporter solicits or desires to collect from its employees.
2.1.4.2 Customer Data of all types that Humanity may include in forms hosted on the Services for the Customer, or may be requested by Customer via customizable fields.
2.1.4.3 Contact and billing details of the Customer's employees, authorized end users, and other business contacts. For example: name, title, employer, contact information (company, email, phone, address, etc.), payment information, and other account-related data.
2.1.4.4 The Customer's users who are authorized by the Customer to access and use the Services.

2.2 Roles of the Parties. The Parties acknowledge and agree that Humanity will Process the Customer Data in the capacity of a Processor and that Customer will be the Controller of the Customer Data. Customer understands that to the extent Third-Party Services are accessed, Customer serves as the Controller and the Third-Party Services are Processors, and the Third-Party Services are not Sub-processors of Humanity.
2.3 Customer Instructions. The Parties agree this DPA and the Agreement constitute Customer's documented instructions regarding Humanity's processing of Customer Data. Humanity will process Customer Data only in accordance with these documented instructions.
2.4 Compliance with Laws. Each party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this DPA, including the GDPR. Humanity is not responsible for determining the requirements of laws applicable to Customer's business or that Humanity's provision of the Services meet the requirements of such laws.

3. Customer's Obligations

3.1 Instructions. Customer shall warrant that the instructions it provides to Humanity pursuant to this DPA comply with the Data Protection Laws.
3.2 Data Subject and Supervisory Authority Requests. The Customer shall be responsible for communications and leading any efforts to comply with all requests made by Data Subjects under the Data Protection Laws, and all communications from Supervisory Authorities that relate to Customer Data, in accordance with Data Protection Laws. To the extent such requests or communications require Humanity's assistance, the Customer shall notify Humanity of the Data Subject or Supervisory Authority request.
3.3 Notice, Consent and Other Authorizations. Customer is responsible for providing the necessary notice to the Data Subjects under the Data Protection Laws. Customer is responsible for obtaining, and demonstrating evidence that it has obtained, all necessary consents, authorizations and required permissions under the Data Protection Laws in a valid manner for Humanity to perform the Services.

4. Humanity's Obligations

4.1 Scope of Processing. Humanity will Process Customer Data on documented instructions from the Customer, and in such manner as is necessary for the provision of Services except as required to comply with a legal obligation to which Humanity is subject. If Humanity believes any documented instruction or additional processing instruction from Customer violates the GDPR or other Data Protection Laws, Humanity will inform Customer without undue delay and may suspend the performance of the Services until Customer has modified or confirmed the lawfulness of the additional processing instruction in writing. Customer acknowledges and agrees that Humanity is not responsible for performing legal research or for providing legal advice to Customer.
4.2 Data Subject Requests. If Humanity receives a request from any Data Subject made under Data Protection relating to Customer Data, Humanity will provide a copy of that request to the Customer within two (2) business days of receipt. Humanity provides Customer with tools to enable Customer to respond to a Data Subjects' requests to exercise their rights under the Data Protection Laws. See https://humanity.com/privacy. To the extent Customer is unable to respond to Data Subject's request using these tools, Humanity will provide reasonable assistance to the Customer in responding to the request.
4.3 Supervisory Authority Requests. Humanity will assist Customer in addressing any communications and abiding by any advice or orders from the Supervisory Authority relating to the Customer Data.
4.4 Retention. Humanity will retain Customer Data only for as long as the Customer deems it necessary for the Permitted Purpose, or as required by applicable laws. At the termination of this DPA, or upon Customer's written request, Humanity will either destroy or return the Customer Data to the Customer, unless legal obligations require storage of the Customer Data.

4.5 Disclosure to Third Parties and Confidentiality.

4.5.1 Humanity will not disclose the Customer Data to third parties except as permitted by this DPA or the Agreement, unless Humanity is required to disclose the Customer Data by applicable laws, in which case Humanity shall (to the extent permitted by law) notify the Customer in writing and liaise with the Customer before complying with such disclosure request.
4.5.2 Humanity treats all Customer Data as strictly confidential and requires all employees, agents, and Sub-processors engaged in Processing the Customer Data to commit themselves to confidentiality, and not Process the Customer Data for any other purposes, except on instructions from Customer.
4.6 Assistance. Taking into account the nature of the Processing and the information available, Humanity will provide assistance to Customer in complying with its obligations under GDPR Articles 32-36 (inclusive) (which address obligations with regard to security, breach notifications, data protection impact assessments, and prior consultation). Upon request, Humanity will provide Customer a list of processing operations.
4.7 Security. Humanity will keep Customer Data confidential and implement and maintain administrative, physical, technical and organizational safeguards for the security (including protection against accidental or unlawful loss, destruction, alteration, damage, unauthorized disclosure of, or access to, Customer Data transmitted, stored or otherwise Processed), confidentiality and integrity of Customer Data as detailed in Annex 1.

5. Contracting with Sub-Processors

5.1 General Consent. Customer agrees that Humanity may engage third-party Sub-processors in connection with the provision of Services, subject to compliance with the requirements below. As a condition to permitting a Sub-processor to Process Customer Data, Humanity will enter into a written agreement with each Sub-processor containing data protection obligations that provide at least the same level of protection for Customer Data as those in this DPA, to the extent applicable to the nature of the Services provided by such Sub-processor. Humanity will provide copies of any Sub-processor agreements to Customer pursuant only upon reasonable request by Customer.

5.2 Current Sub-processor List. Customer acknowledges and agrees that Humanity may engage its current Sub-processors listed here.
5.3 Written Notice Via Mailing List. Humanity will provide Customer with notice (“New Sub-processor Notice”) of the addition of any new Sub-processor to the Sub- processor List at any time during the term of the Agreement. Humanity will provide Customer with additional information about any Sub-processor on the Sub-processor List that Customer may reasonably request upon receipt of a New Sub-processor Notice
5.4 Customer Objection. If Customer has a reasonable basis to object to Humanity’s use of a new Sub-processor, Customer will notify Humanity promptly in writing within 15 days after receipt of a New Sub-processor Notice. Humanity will use reasonable efforts to make available to Customer a change in the affected Services or recommend a commercially reasonable change to Customer’s configuration or use of the affected Services to avoid processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If Humanity is unable to make available such change within a reasonable period of time, which will not exceed 30 days, Customer may terminate the portion of any Agreement relating to the Services that cannot be reasonably provided without the objected-to new Sub-processor by providing written notice to Humanity.
5.5 Responsibility. Humanity will remain responsible for its compliance with the obligations of this DPA and for any acts and omissions of its Sub-processors that cause Humanity to breach any of Humanity’s obligations under this DPA.

6. Security Incident Management

6.1 Notification. Humanity shall, to the extent permitted by law, notify Customer without undue delay, but no later than 48 hours after becoming aware of any Security Incident.
6.2 Security Incident. Humanity’s notification of a Security Incident to the Customer to the extent known should include: (a) the nature of the incident; (b) the date and time upon which the incident took place and was discovered; (c) the number of data subjects affected by the incident; (d) the categories of Customer Data involved; (e) the measures – such as encryption, or other technical or organizational measures – that were taken to address the incident, including measures to mitigate the possible adverse effects; (f) whether such proposed measures would result in a disproportionate effort given the nature of the incident; (g) the name and contact details of the data protection officer or other contact; and (h) a description of the likely consequences of the incident. The Customer alone may notify any public authority.

7. Transfers Outside the European Economic Area

7.1 Privacy Shield. Humanity complies with the terms of the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, and is Privacy Shield certified. That certification will serve as the transfer mechanisms for any Customer transfers of Customer Data under this DPA to Humanity from the EEA, Switzerland or the United Kingdom to the United States. The Parties acknowledge and agree that on the request of the United States Department of Commerce (or any successor body) or a competent supervisory authority, enforcement or other public or regulatory authority, court or tribunal, Humanity may make available to them a summary or representative copy of this DPA or any relevant provisions in the Agreement.
7.2 Standard Contractual Clauses. To the extent Privacy Shield is nullified or no longer is recognized by the European Commission as a valid transfer mechanism, the Parties agree the Standard Contractual Clauses (as evidence by each party’s authorized signature on the Agreement), will apply to Customer Data that is transferred outside the EEA, either directly or via onward transfer, to any country not recognized by the European Commission as providing as adequate level of protection for personal data (as described by the GDPR.
7.2.1. Pursuant to Clause 5(h) of the Standard Contractual Clauses, Customer acknowledges and expressly agrees Humanity may engage new Sub-processors as described in Section 5 of this DPA.
7.2.2 The Parties agree the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out as described in Section 8 of this DPA.
7.2.3 The Parties agree that the certification of deletion of Customer Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Humanity to Customer only upon Customer’s request.

8. THIRD PARTY CERTIFICATIONS AND AUDITS

8.1 Certification/SOC Report. In addition to the information contained in this DPA, upon Customer’s request, and subject to the confidentiality obligations set forth in the Agreement place, Humanity will make available the following documents and information regarding the System and Organization Controls (SOC) 2 Report (or the reports or other documentation describing the controls implemented by Humanity that replace or are substantially equivalent to the SOC 2), so that Customer can reasonably verify Humanity’s compliance with its obligations under this DPA.
8.2 Audits. To the extent the reports provided in Section 8.1 do not verify Humanity’s compliance with its obligations under this DPA, Customer may audit Humanity’s compliance with this DPA up to once per year, unless requested by a Supervisory Authority or in the event of a Security Incident. Such audit will be conducted by an independent third party (“Auditor”) reasonably acceptable to Humanity. Before the commencement of any such on-site audit, Customer must submit a detailed proposed audit plan to Humanity at least two weeks in advance of the proposed audit date. The proposed audit plan must describe the proposed scope, duration and state date of the audit. Humanity will review the proposed audit plan and provide Customer with any concerns or questions. Humanity will work cooperatively with Customer to agree on a final audit plan. The results of the inspection and all information reviewed during such inspection will be deemed Humanity’s confidential information and shall be protected by Auditor in accordance with the confidentiality provisions noted above. Notwithstanding any other terms, the Auditor may only disclose to the Customer specific violations of the DPA, if any, and the basis for such findings, and shall not disclose to Customer any of the records or information reviewed during the inspection.

9. Miscellaneous

9.1 Obligations Post-termination. Termination or expiration of this DPA shall not discharge the Parties from their obligations meant to survive the termination or expiration of this DPA.
9.2 Severability. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invaliding the remaining provisions hereof, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. The Parties will attempt to agree upon a valid and enforceable provision that is a reasonable substitute and shall incorporate such substitute provision into this DPA.

The parties' authorized signatories have duly executed this DPA:

CUSTOMER
Name (written out in full):
Title:
Address:

Signature…………………………………………

HUMANITY.COM, INC.
Name (written out in full): David Charron
Title: Vice President Strategy and Legal Affairs
Address: 2121 N. California Blvd. Suite 290
Walnut Creek, CA 94596
Other information necessary in order for the contract to be binding (if any)

David Charron
Signature…………………………………………

Annex 1 Security Policies, Procedures, Controls

Humanity implements the following security measures with respect to the Customer Data:
1. Access Control of Processing Areas. Processes to prevent unauthorized persons from gaining access to the Humanity data processing equipment (namely telephones, database and application servers and related hardware) where the Customer Data are processed or used, to include:
a. establishing security areas;
b. protection and restriction of access paths;
c. securing the data processing equipment and personal computers;
d. establishing access authorization for employees and third parties, including respective authorization;
e. all access to the data centers where Customer Data are hosted is logged, monitored, and tracked; and
f. the data centers where Customer Data are hosted is secured by a security alarm system, and other appropriate security measures.
2. Access Control to Data Processing Systems. Processes to prevent Humanity data processing systems from being used by unauthorized persons, to include:
a. identification of the terminal and/or the terminal user to the data processor systems;
b. automatic time-out of user terminal if left idle, identification and password required to reopen;
c. regular examination of security risks by internal personnel and qualified third-parties;
d. issuing and safeguarding of identification codes;
e. password complexity requirements (minimum length, expiry of passwords, etc.); and
f. protection against external access by means of firewall and network access controls.
3. Access Control to Use Specific Areas of Data Processing Systems. Measures to ensure that persons entitled to use Humanity data processing systems are only able to access the data within the scope and to the extent covered by their respective access permission (authorization) and that Customer Data cannot be read, copied or modified or removed without authorization, to include by:
a. implementing binding employee policies and providing training in respect of each employee's access rights to the Customer Data;
b. assignment of unique user identifiers with permissions appropriate to the role;
c. effective and measured disciplinary action against individuals who access Personal Data without authorization;
d. release of data to only authorized persons; and
e. policies controlling the retention of back-up copies.
4. Transmission Control. Procedures to prevent Customer Data from being read, copied, altered or deleted by unauthorized parties during the transmission thereof or during the transport of the data media and to ensure that it is possible to check and establish to which bodies the transfer of Customer Data by means of data transmission facilities is envisaged, to include:
a. use of firewall and encryption technologies to protect the gateways and pipelines through which the data travels;
b. implementation of encrypted connections to safeguard the connection to Humanity systems;
c. constant monitoring of infrastructure (e.g. ICMP-Ping at network level, disk space examination at system level, successful delivery of specified test pages at application level); and
d. monitoring of the completeness and correctness of the transfer of data (end-to-end check).

5. Input Control. Measures to ensure that it is possible to check and establish whether and by whom Customer Data has been input into data processing systems or removed, to include:
a. authentication of the authorized personnel;
b. protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data;
c. Segregation and protection of stored data via database schemas and logical access controls;
d. utilization of user codes (passwords);
e. proof established within data importer’s organization of the input authorization; and
f. providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are capable of being locked.

6. Availability Control. Measures to ensure that Customer Data are protected from accidental destruction or loss, to include:
a. automatic failover between sites;
b. infrastructure redundancy; and
c.regular backups performed on database servers.

7. Segregation of Processing. Procedures to ensure that data collected for different purposes can be processed separately, to include:
a. separating data through application security for the appropriate users;
b. storing data, at the database level, in different tables, separated by the module or function they support; and
c. designing interfaces, batch processes and reports for only specific purposes and functions, so data collected for specific purposes is processed separately.

Annex 2 Standard Contractual Clauses

(processors)
For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of data exporting organization:	Customer and contact information identified in the HUMANITY Order Form

The data exporting organization identified in the table above (**the “data exporter”)**
– And –

Name of data importing organization:	Humanity.com, Inc.
Address:	2121 N. California Blvd. Suite 290 Walnut Creek, CA. 94596
Tel.:	+1-888-973-6030
E-mail:	legal-notices@Humanity.com

(**the “data importer”**)
each a “party”; together “the parties”,
HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:
1. *'**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;
2. '***the data exporter'*** means the controller who transfers the personal data;
3. ***'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;
4. *'**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;
5. **'*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;
6. *'**technical and organizational security measures'*** means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2
Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the 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 organizational security measures specified in Appendix 2 to this contract;
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, unauthorized 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 organizational 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 unauthorized access, and
c. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized 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 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data

exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7
Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against 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.
c. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9
Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10
Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11
Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.
2. The prior written contract between the data importer and the sub-processor shall also provide for a third- party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On Behalf of the data exporter:
Name (written out in full):
Title:
Address:
Other information necessary in order for the contract to be binding (if any)
Signature………………………………………….

On Behalf of the data importer:
Name (written out in full): David Charron
Title: Vice-President, Strategy and Legal Affairs
Address: 2121 N. California Blvd. Suite 290 ,Walnut Creek, CA. 94596
Other information necessary in order for the contract to be binding (if any)
David Charron
Signature………………………………………….

APPENDIX 1 to The Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.
The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.
Capitalized terms used in this Appendix which are otherwise undefined in these Clauses have the meanings given to them in the Data Processing Agreement to which these Clauses are attached.

Data exporter

The data exporter is ……………………………………………... and the legal entity that has executed the Standard Contractual Clauses as a data exporter and has purchased Services on the basis of one or more Agreements with Humanity.

Data importer

The data importer is a Humanity.com which is a provider of workforce management and employee scheduling software services to its customers.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify): Data subjects include:

- Natural persons who submit personal data to the data importer via use of the Services (employment related information).
- Natural persons who are employees, representatives, or other business contacts of the exporter.
- The data exporter's users who are authorized by the data exporter to access and use the Services.

Categories of data

The personal data transferred concern the following categories of data (please specify): The data exporter may submit Personal Data to the Services, and may request for its employees to submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, without limitation:

- Personal Data of all types that may be submitted by employees to the data exporter via user of the Services. For example: name, work location, age, contact details, position/title, gender, salary and other preferences and other personal details that the data exporter solicits or desires to collect from its employees for the purpose of scheduling them to mutually agreeable work schedules
- Personal Data of all types that the data importer may include in forms hosted on the Services for the data exporter
- Contact and billing details of the data exporter's employees, authorized end users, and other business contacts. For example: name, title, employer, contact information (company, email, phone, address, etc.), payment information, and other account-related data.

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify): All special categories of personal data as defined by Data Protection Law.
Processing Operations
The personal data transferred will be subject to the following basic processing activities (please specify): For the purposes of delivering the Services (including administration, operations, technical and customer support), the data set out above will be routinely accessed from the data importer's systems, which are based outside of the European Economic Area.

DATA EXPORTER

Name:......................................

Authorised Signature:..

DATA IMPORTER

Name: David Charron

David Charron

Authorised Signature:..

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.
Capitalized terms used in this Appendix which are otherwise undefined in these Clauses have the meanings given to them in the Data Processing Agreement to which these Clauses are attached.
Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):
The Service Provider will implement and maintain technical and organisational security measures aimed at protecting Customer Data against a personal data breach or other accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, and shall include without limitation: (i) securing business facilities, data centers, paper files, servers, back-up systems and computing equipment; (ii) implementing network, device application, database and platform security; (iii) implementing and maintaining incident response policies and data retention policies for Customer Data; (iv) implementing authentication and access controls within media, applications, operating systems and equipment; (v) encrypting Customer Data transmitted over public or wireless networks; (vi) strictly segregating Customer Data from information of the Service Provider or its other customers; and (vii) implementing appropriate personnel security and integrity procedures and practices.

DATA EXPORTER

Name:......................................

Authorised Signature:..

DATA IMPORTER

Name: David Charron

David Charron

Authorised Signature:..