Data Processing Addendum (GDPR 2021 Standard Contractual Clauses)

This Data Processing Addendum ("DPA") supplements the Agreement between Humanity.com, Inc. ("Humanity", a subsidiary of TimeClock Plus, LLC ("TCP")) 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 December 19th, 2022. Humanity reserves the right to periodically update and modify this DPA, and such modification will automatically become effective in the next service term. Latest DPA version is 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 "Model Clauses" attached at Annex 2, means the standard contractual clauses annexed to the EU Commission Decision 2021/914/EU of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (transfers from controller to processor), as may be amended, superseded or replaced from time to time.
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 Details of Processing.
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://tcpsoftware.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 in **ANNEX III** below **,** “LIST OF SUB-PROCESSORS”.
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 72 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 The Parties agree that 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 SOC 2 Report. In addition to the information contained in this DPA, upon written Customer's request, and subject to the confidentiality obligations set forth under a signed NDA, Humanity will make available an independent third party ("Auditor") SOC 2 report under AICPA's Trust Principles of Security, Availability, Confidentiality, and Processing Integrity, 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 request to 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. (a subsidiary of TimeClock Plus, LLC ("TCP"))
Name (written out in full): Derek McIntyre
Title: COO
Address: 1 TimeClock Dr. San Angelo, Texas, 76904
Other information necessary in order for the contract to be binding (if any)
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 2021 STANDARD CONTRACTUAL CLAUSES (FOR EU/EEA AND SWISS DATA EXPORTERS)

SECTION I

Clause 1- Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2- Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3- Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 –Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 –Clause 9(a), (c), (d) and (e);

(iv) Clause 12 –Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4- Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5- Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6- Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8- Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter ‘personal data breach’). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter ‘sensitive data’), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (4) (in the same country as the data importer or in another third country, hereinafter ‘onward transfer’) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

§(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9 - Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least one month in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10 - Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11 - Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 - Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13 - Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15 - Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16 - Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17 - Governing law

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18 - Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of Ireland.

Data Importer HUMANITY.COM INC (Provider) **(a subsidiary of TimeClock Plus, LLC (“TCP”)).**	**Data Exporter:**
________________________ **Signature**	________________________ **Signature**
________________________ **Name:**	________________________ **Name:**
________________________ **Title/Position:**	________________________ **Title/Position:**

ANNEX I TO THE 2021 STANDARD CONTRACTUAL CLAUSES

A. LIST OF PARTIES

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

Name:

Address:

Contact person’s name, position and contact details:

Activities relevant to the data transferred under these Clauses: …………………………………………………………………

Signature and date: ……………………………

Role (controller/processor): Controller

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

Name: **HUMANITY.COM INC (a subsidiary of TimeClock Plus, LLC (“TCP”))**

Address: See as specified in the Data Processing Agreement.

Contact person’s name, position and contact details: See as specified in the Data Processing Agreement.

Activities relevant to the data transferred under these Clauses: SaaS Cloud based solution for employee scheduling

Signature and date: ……………………………

Role (controler/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

PII (Personal identifiable information)

Categories of personal data transferred

Only full name and email address is necessary for account opening in Humanity application.

Sensitive data transferred and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

N/A

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Data can be transferred in one-off or on a continuous basis.

Nature of the processing

For scheduling purposes.

Purpose(s) of the data transfer and further processing

For scheduling purposes.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Customer data is held in our systems only while the account is active, and some data is held for longer (e.g. IP addresses of client access, audit logs, invoices…), due to legal requirements. When the account is canceled, customers PII data is held in our application up to 45 days.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Specified in detailed in ANNEX III.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authorities in accordance with Clause 13

Humanity has further committed to refer unresolved privacy complaints under the Privacy Shield Principles to an independent dispute resolution mechanism, the BBB EU PRIVACY SHIELD, operated by BBB National Programs. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit https://bbbprograms.org/privacy-shield-complaints for more information and to file a complaint. This service is provided free of charge to you.

ANNEX II TO THE 2021 STANDARD CONTRACTUAL CLAUSES

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Humanity has audited for SOC II Type I, to ensure that all technical and organisational controls are in place to ensure an appropriate level of security, considering the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

SOC II Type I report can be requested from our compliance team under NDA (compliance@tcpsoftware.com)

ANNEX III TO THE 2021 STANDARD CONTRACTUAL CLAUSES

LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

SUB-PROCESSOR NAME	COUNTRY	KEY FUNCTIONS
Amazon Web Services (AWS)	US	IaaS and SaaS provider, for live (production) and development environments, for storing backups, file storage and Lambda functions
Intercom	US	to distribute product-related information
Zoom	US	to communicate with customers
SalesForce	US	to unite our Sales and Support efforts and to improve and simplify communication with our customers and trials
Outreach	US	used to improve and simplify communication with our customers and trials
Segment	US	used for better understanding of customer journeys across Humanity website and application
Microsoft O365	US	internal company's mail and document store system

LogEntries	US	for system log processing
Crashlytics	US	bug tracking and analytics
FireBase	US	crash analytics tool
Sentry.io	US	error tracking and application health monitoring
Zuora	US	integrations partner - for billing/payment processing/subscription tracking
Mongo	US	application logging tool. Store data for 30 days
Matillion	US	data integration tools used to extract, transform and load data into company's AWS account (Amazon Redshift & S3).
Pentaho	US	data integration tools used to extract, transform and load data into company's AWS account (Amazon Redshift & S3).
Amazon RedShift	US	our Data Warehouse provider
Clair	US	Clair offers a platform that allows our customers (end users) to open spending and savings bank account. Clair advances a portion of wages for free to certain user's accounts, allowing them to access those wages in advance of receiving their paycheck.

Data Importer HUMANITY.COM INC (Provider) (a subsidiary of TimeClock Plus, LLC ("TCP")).

____
Signature

____
Name:

____
Title/Position:

Data Exporter:

____
Signature

____
Name:

____
Title/Position: