Humanity

DATA PROCESSING ADDENDUM

Effective Date: 25th of May 2018

This Data Processing Addendum ("**DPA**") is made as of the Effective Date by and between Humanity.com Inc. ("Humanity"), and Customer, pursuant to the Master Humanity SaaS Subscription Agreement or the Subscription Terms of Service, as applicable ("Agreement").

This DPA overrides any previous Humanity data processing agreement and may only be varied in writing by and at the instigation of Humanity, or by agreement between Humanity and a client, should the performance of the DPA be then operative between Humanity and a particular client.

This DPA amends the Agreement and sets out the terms that apply when Personal Data is processed by Humanity under the Agreement. The purpose of the DPA is to ensure such processing is conducted in accordance with applicable laws and with due respect for the rights and freedoms of individuals whose Personal Data are processed. Other capitalized terms used but not defined in this DPA have the same meanings as set out in the Agreement.

1. Definitions

1.1. For the purposes of this DPA:

a) "EEA" means the European Economic Area, which constitutes the member states of the European Union, the United Kingdom, Norway, Iceland and Liechtenstein.
b) "EU Data Protection Legislation" means (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, including any applicable national implementations of it; and (ii) on and after 25 May 2018, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (as amended, replaced or superseded) ("GDPR");
c) "Controller" shall mean the entity which, alone or jointly with others, determines the purposes and means of the processing of Personal Data;
d) "Processor" shall mean an entity which processes Personal Data on behalf of the Controller;
e) "Personal Data" means any information relating to an identified or identifiable individual where such information is contained within Customer Data and is protected similarly as personal data or personally identifiable information under applicable Data Protection Law.
f) "Data Subject" means the individual to whom Personal Data relates.
g) "Instruction" means the written, documented instruction, issued by Controller to Processor, and directing the same to perform a specific action with regard to Personal Data (including, but not limited to, depersonalizing, blocking, deletion, making available).

h) **“Personal Data Breach”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
i) **“Processing”** means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data.

2. Details of the Processing

2.1. Categories of Data Subjects

Controller’s Contacts and other end users including Controller’s employees, contractors, collaborators, customers, prospects, suppliers and subcontractors. Data Subjects also include individuals attempting to communicate with or transfer Personal Data to the Controller’s end users.

2.2. Types of Personal Data

Contact Information, the extent of which is determined and controlled by the Customer in its sole discretion, and other Personal Data such as navigational data (including website usage information), email data, system usage data, application integration data, and other electronic data submitted, stored, sent, or received by end users via the Service.

2.3. Subject-Matter and Nature of the Processing

The subject-matter of Processing of Personal Data by Processor is the provision of the services to the Controller that involves the Processing of Personal Data. Personal Data will be subject to those Processing activities as may be specified in this DPA and an Order.

2.4. Purpose of the Processing

Personal Data will be Processed for purposes of providing the services set out and otherwise agreed to in the Terms of Service and this DPA.

2.5. Duration of the Processing

Personal Data will be Processed for the duration of this DPA, subject to Section 4 of this DPA.

3. Roles and Customer responsibility

3.1. Parties' Roles

To the extent that Humanity processes Personal Data in the course of providing the Services, it will do so only as a Processor acting on behalf of Customer (as Controller) and in accordance with the requirements of the Agreement.

3.2. Purpose Limitation

Humanity will process the Personal Data only for the purpose of providing the Services and in accordance with Controller’s lawful instructions.

3.3. Scope

Within the scope of this DPA and in its use of the services, Controller shall be solely responsible for complying with the statutory requirements relating to data protection and privacy, in particular regarding the disclosure and transfer of Personal Data to the Processor and the Processing of Personal Data. For the avoidance of doubt, Controller’s instructions for the Processing of Personal Data shall comply with the Data Protection Law. This DPA is Customer’s complete and final instruction to Humanity in relation to Personal Data and that additional instructions outside the scope of DPA would require prior written agreement between the parties. Instructions shall initially be specified in this DPA and may, from time to time thereafter, be amended, amplified or replaced by Controller in separate written instructions (as individual instructions).

3.3. Compliance

Customer, as Controller, shall be responsible for ensuring that: a) it has complied, and will continue to comply, with all applicable laws relating to privacy and data protection, including EU Data Protection Legislation; and b) it has, and will continue to have, the right to transfer, or provide access to, the Personal Data to Humanity for processing in accordance with the terms of the Agreement and this DPA.

3.4. Controller shall inform Processor without undue delay and comprehensively about any errors or irregularities related to statutory provisions on the Processing of Personal Data.

4. Applicability of DPA

4.1. This DPA will apply only to the extent that Humanity processes Personal Data from the EEA on behalf of the Customer.

4.2 GDPR

The parties agree that Exhibits A and B to this DPA will apply only on and after 25 May 2018. Where the GDPR materially or adversely impacts Humanity's continued provision of the Services (including its costs in providing the Services) and / or Customer's receipt of the Services, the Parties shall discuss in good faith and acting reasonably what changes may be necessary and operationally, technically and commercially feasible to the Agreement and/or the DPA and/or the Services (including, without limitation, the fees payable by Customer to Humanity for the Services) in order to enable Humanity to continue providing the Services. No such changes shall be effective unless agreed between the Parties pursuant to this Clause.

5. Obligations of Processor

5.1. Compliance with Instructions

5.1.1. The parties acknowledge and agree that Customer is the Controller of Personal Data and Humanity is the Processor of that data. Processor shall collect, process and use Personal Data only within the scope of Controller’s Instructions. If the Processor believes that an Instruction of the Controller infringes the Data Protection Law, it shall immediately inform the Controller without delay. If Processor cannot process Personal Data in accordance with the Instructions due to a legal requirement under any applicable European Union or Member State law, Processor will (i) promptly notify the Controller of that legal requirement before the relevant Processing to the extent permitted by the Data Protection Law; and (ii) cease all Processing (other than merely storing and maintaining the security of the affected Personal Data) until such time as the Controller issues new instructions with which Processor is able to comply. If this provision is invoked, Processor will not be liable to the Controller under this DPA for any failure to perform the applicable services until such time as the Controller issues new instructions in regard to the Processing.

5.2. Security

5.2.1. Processor shall take the appropriate technical and organisational measures to adequately protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data. Such measures include, but are not be limited to:

- the prevention of unauthorised persons from gaining access to Personal Data Processing systems (physical access control),
- the prevention of Personal Data Processing systems from being used without authorisation (logical access control),
- ensuring that persons entitled to use a Personal Data Processing system gain access only to such Personal Data as they are entitled to accessing in accordance with their access rights, and that, in the course of Processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorisation (data access control),

- ensuring that Personal Data cannot be read, copied, modified or deleted without authorisation during electronic transmission, transport or storage on storage media, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified (data transfer control),
- ensuring the establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in, or removed from Personal Data Processing systems (entry control),
- ensuring that Personal Data is Processed solely in accordance with the Instructions (control of instructions),
- ensuring that Personal Data is protected against accidental destruction or loss (availability control).

5.2.2. Upon Controller's request, Processor shall provide a current Personal Data protection and security program relating to the Processing hereunder.

5.2.3. Processor will facilitate Controller's compliance with the Controller's obligation to implement security measures with respect to Personal Data (including if applicable Controller's obligations pursuant to Articles 32 to 34 (inclusive) of the GDPR), by (i) implementing and maintaining security measures, (ii) complying with the terms of Section ”Personal Data Breaches”; and (iii) providing the Controller with information in relation to the Processing in accordance with Section ”Audits”.

5.3. Confidentiality

5.3.1. Processor shall ensure that any personnel whom Processor authorises to process Personal Data on its behalf is subject to confidentiality obligations with respect to that Personal Data. The undertaking to confidentiality shall continue after the termination of the above-entitled activities.

5.4. Personal Data Breaches

5.4.1. Processor will notify the Controller as soon as practicable after it becomes aware of any of any Personal Data Breach affecting any Personal Data. At the Controller's request, Processor will promptly provide the Controller with all reasonable assistance necessary to enable the Controller to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if Controller is required to do so under the Data Protection Law.

5.5. Data Subject Requests

5.5.1. Processor will provide reasonable assistance, including by appropriate technical and organisational measures and taking into account the nature of the Processing, to enable Controller to respond to any request from Data Subjects seeking to exercise their rights under the Data Protection Law with respect to Personal Data (including access, rectification, restriction, deletion or portability of Personal Data, as applicable), to the extent permitted by the law. If such request is made directly to Processor, Processor will promptly inform Controller and will advise Data Subjects to submit their request to the Controller. Controller shall be solely responsible for responding to any Data Subjects' requests. Controller shall reimburse Processor for the costs arising from this assistance.

5.6. Sub-Processors

5.6.1. To support delivery of our Services, Humanity may engage and use data processors with access to certain Customer Data (each, a "Sub-Processor"). This page provides important information about the identity, location and role of each Sub-Processor. Terms used on this page but not defined have the meaning set forth in the Terms of Use or superseding written agreement between Customer and Humanity (the "Agreement").

5.6.2. Humanity currently uses third party Sub-Processors to provide infrastructure services, and to help us provide customer support and email notifications. Prior to engaging any third party Sub-Processor, Humanity performs diligence to evaluate their privacy, security and confidentiality practices, and executes an agreement implementing its applicable obligations.

5.6.3. Humanity shall be entitled to engage sub-Processors to fulfil Processor's obligations defined in this DPA only with Controller's written consent. For these purposes, Controller consents to the engagement as sub-Processors of Processor's affiliated companies and third parties.

5.6.4. If Humanity intends to instruct sub-Processors, it will notify the Controller thereof in writing (email to the email addresses) on record in Processor's account (information for Controller is sufficient) and will give the Controller the opportunity to object to the engagement of the new sub-Processors within 30 days after being notified. The objection must be based on reasonable grounds (e.g. if the Controller proves that significant risks for the protection of its Personal Data exist at the sub-Processor). If the Processor and Controller are unable to resolve such objection, either party may terminate this DPA by providing written notice to the other party. Controller shall receive a refund of any prepaid but unused fees for the period following the effective date of termination.

5.6.5. Where Processor engages sub-Processors, Processor will enter into a contract with the sub-Processor that imposes on the sub-Processor the same obligations that apply to Processor under this DPA. Where the sub-Processor fails to fulfil its data protection obligations, Processor will remain liable to the Controller for the performance of such sub-Processors obligations.

5.6.6. Where a sub-Processor is engaged, the Controller must be granted the right to monitor and inspect the sub-Processor's activities in accordance with this DPA and the Data Protection Law, including to obtain information from the Processor, upon written request, on the substance of the contract and the implementation of the data protection obligations under the sub-Processing contract, where necessary by inspecting the relevant contract documents.

5.6.7. The provisions of this Section shall mutually apply if the Processor engages a sub-Processor in a country outside the European Economic Area ("EEA") not recognised by the European Commission as providing an adequate level of protection for personal data. If, in the performance of this DPA, Humanity transfers any Personal Data to a sub-processor located outside of the EEA, Humanity shall, in advance of any such transfer, ensure that a legal mechanism to achieve adequacy in respect of that processing is in place.

5.6.8. Sub-Processors list:

Entity Name	Subprocessing Activities	Entity Country
IBM Cloud (IBM)	Cloud Service Provider	United States
Google Inc.	Cloud Service Provider	United States
Amazon Web Services, Inc.	Cloud Service Provider	United States
Hetzner Online GmbH	Cloud Service Provider	Germany
Google Inc.	Cloud-based Service Provider	United States
Rapid7 LLC.	Cloud-based Logging Services	United States
Salesforce.com, Inc.	Cloud-based CRM services	United States
Zendesk, Inc.	Cloud-based Customer Support Services	United States
The Rocket Science Group, LLC	Cloud-based marketing supporting services	United States
APIHub, Inc.	Cloud-based sales and marketing supporting services	United States
Intercom, Inc.	Cloud-based marketing customer supporting services	United States
Wingify Software Private Limited	Cloud-based website analytics services	India
Segment.io, Inc.	Cloud-based customer data analytics services	United States
Google Inc. (Crashlytics)	Cloud-based application performance monitoring services	United States
ZFERRAL, INC.	Cloud-based referral and affiliate services	United States
Twilio Inc.	Cloud-based messaging and notification services	United States
Functional Software, Inc.	Cloud-based application error tracking services	United States
Slack Technologies, Inc.	Cloud-based integrated team communication services	United States
Zuora, Inc.	Cloud-based subscription management system	United States
PayPal Holdings, Inc.	Cloud-based payment service provider	United States
Stripe, Inc.	Cloud-based payment service provider	United States

Data Integration Partners

Humanity may use the following Sub-Processors as both service providers and data integration partners:

Entity Name	Subprocessing Activities	Entity Country
Cloud Elements Inc.	Cloud-based Data Integration Support Services	United States

5.6.9. Transfers to subsequent third parties are covered by the service agreements with our Customers (the Controller). Furthermore, Humanity supports End Users' rights to retrieve any information retained on our servers which relates to such End User. Humanity acknowledges that you have the right to access your Personal Information. We have processes in place to accommodate an End User's rights to delete data, amend erroneous data, access data and receive Personal Data or Sensitive Data in a machine readable commonly used format, all subject to reasonable technical restrains and abilities.

5.6.10. Personal Information or Personal Data is information by which an individual may be personally identified, including name, address, e-mail address, telephone number or any other information that is defined as Personal Information, Personal Data, or Personally Identifiable Information under an applicable law (hereinafter referred to as *"Personal Information"*)

5.6.11. Users are not obligated to provide us with any information by law. However, we require certain information in order to provide our services properly. Under some jurisdictions (such as under certain E.U. regulations), a User has a right to withdraw its consent at any time. In such a case, the withdrawal will not affect the lawfulness of processing based on consent before its withdrawal.

5.6.12. Please note that consent for the gathering and processing of data for one Service does not automatically mean that a User consents to the processing of data in connection with other Services. Our Customer (Data Controller) should always make sure that the User's consent is relevant, clear, valid, and to the extent reasonably possible, not "bundled" with any other written agreement (especially if required under applicable laws), unambiguous and if required under applicable law, affirmative and active (meaning not by virtue of any inaction).

5.6.13. Humanity aims to process only adequate, accurate and relevant data limited to the needs and purposes for which it is gathered. It also aims to store data for the time period necessary to fulfill the purpose for which the data is gathered. Humanity only collects data in connection with a specific legitimate purpose.

5.7. Data Transfers

5.7.1. Controller acknowledges and agrees that, in connection with the performance of the services under this DPA, Personal Data will be transferred to Humanity in United States of America. Humanity is compliant with the directives regarding Personal Data protection in the United States, and is implementing appropriate safeguards for such transfers, pursuant to Article 46 of the GDPR.

5.8. Deletion or Retrieval of Personal Data

5.8.1. Other than to the extent required to comply with Data Protection Law, following termination or expiry of this DPA, Processor will delete all Personal Data (including copies thereof) processed pursuant to this DPA. If Processor is unable to delete Personal Data for technical or other reasons, Processor will apply measures to ensure that Personal Data is blocked from any further Processing.

5.8.2. Controller shall, upon termination or expiration of this DPA and by way of issuing an Instruction, stipulate, within a period of time set by Processor, the reasonable measures to return data or to delete stored data. Any additional cost arising in connection with the return or deletion of Personal Data after the termination or expiration of this DPA shall be borne by Controller.

6. Audits

6.1. Controller may, prior to the commencement of Processing, and at regular intervals thereafter, audit the technical and organisational measures taken by Processor.
For such purpose, Controller may:

- obtain information from the Processor,
- request Processor to submit to Controller an existing attestation or certificate by an independent professional expert,
- upon reasonable and timely advance agreement, during regular business hours and without interrupting Processor's business operations, conduct an on-site inspection of Processor's business operations or have the same conducted by a qualified third party which shall not be a competitor of Processor.

6.2. Processor shall, upon Controller's written request and within a reasonable period of time, provide Controller with all information necessary for such audit, to the extent that such information is within Processor's control and Processor is not precluded from disclosing it by applicable law, a duty of confidentiality, or any other obligation owed to a third party.

7. Data Privacy, Security & Confidentiality

7.1. We take great care in implementing, enforcing and maintaining the security of our Services, Site and Users' information, also complying to the EU General Data Protection Regulation (Released April 6, 2016).

7.2. Humanity understands that the service provided can capture a wide range of information and may be highly sensitive, confidential or proprietary. Humanity values the trust that our customers, whether they be individuals or large organisations, place in us by letting us be the custodians of their personal data.
Humanity implements, enforces and maintains security policies to prevent the unauthorized or accidental access to or destruction, loss, modification, use or disclosure of Personal

Information or Personal Data and to monitor compliance of such policies on an ongoing basis.

7.3. Our Privacy Policy details how we handle your data that we encourage you to review. We aim to be transparent regarding our privacy practices so that there are no surprises with what happens with your data. We will not use your service, or the information collected from your services, in any way other than as described in our Privacy Policy. We will make every effort to ensure that whatever information you provide will be maintained in a secure environment. We also encourage all stakeholders to engage in good privacy practices with respect their data.

7.4. Humanity takes our users' security and privacy concerns seriously. We strive to ensure that user data is kept secure, and that we collect only as much personal data as is required to make our users' experience with Humanity as efficient and satisfying as possible. We also aim to collect data in the most unobtrusive manner possible. We aim to be transparent about our security infrastructure and practices to help reassure you that your data is sufficiently protected.

7.5. Prior to releasing application features, updates or patches, we perform regular application code scans against potential security issues and engage independent contractors specialized in vulnerability assessment and penetration testing of our development and production environments.

7.6. Our website and also our application supporting infrastructure is hosted by IBM Cloud, a cloud hosting provider from United States of America (U.S.A.), which provides advanced security features and is compliant with most relevant information security industry standards and best practices. We perform regular data backups, encrypt and store them using another cloud provider's services - Amazon Web Services (AWS), also based in U.S.A. and compliant with most relevant information security industry standards and best practices.

7.7. All information is stored with logical separation from information of other Customers. However, we do not guarantee that unauthorized access will never occur.

7.8. We use a combination of processes, technology and physical security controls to help protect Personal Information and Personal Data from unauthorized access, use, or disclosure. When Personal Information or Personal Data is transferred over the Internet, we encrypt it using Transfer Layer Security (TLS) encryption technology or similar technology. Each server is protected by a firewall, exposing it only to the minimum ports necessary. However, no security controls are 100% effective, and we cannot completely ensure or warrant the security of your Personal Information and Personal Data.

7.9. Unless otherwise agreed with the Customer and subject to applicable law, Humanity shall act in accordance with its policies to promptly notify Customer in the event that any Personal Information or Personal Data processed by Humanity on behalf of a Customer is lost, stolen, or where there has been any unauthorized access to it.

7.10. Humanity uses third party vendors and hosting partners to provide the necessary hardware, software, networking, storage, and related technology required to run the Humanity Services. Where practical, we seek to obtain confidentiality agreements that are consistent with this Privacy Policy and that limit others' use or disclosure of your Personal Information and Personal Information.

8. Access Control

Preventing Unauthorised Access

8.1. Outsourced processing:

As previously stated, Humanity may host its Service with outsourced cloud infrastructure providers. Additionally, Humanity maintains contractual relationships with vendors in order to provide the Service in accordance with our Data Processing Agreement. Humanity relies on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

8.2. Physical and environmental security:

Humanity may host its infrastructure with multi-tenant, outsourced infrastructure providers. The physical and environmental security controls are audited for ISO 27001 compliance, among other certifications.
Authentication: Humanity implemented a uniform password policy for its customer services. Customers who interact with the services via the user interface must authenticate before accessing non-public customer data.

8.3. Authorisation:

Customer data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorisation model in each of Humanity's services is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customisation options. Authorisation to data sets is performed through validating the user's permissions against the attributes associated with each data set.

8.4. Application Programming Interface (API) access:

Public APIs may be accessed using an API key or through OAuth authorisation.

Preventing Unauthorised services Use

8.5. Humanity implements industry standard access controls and detection capabilities for the internal networks that support its services.

8.6. Access controls:

Network access control mechanisms are designed to prevent network traffic using unauthorised protocols from reaching the infrastructure. The technical measures implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.

8.7. Intrusion detection and prevention:

Humanity implemented a Web Application Firewall (WAF) solution to protect Humanity services and other internet-accessible applications. The WAF is designed to identify and prevent attacks against publicly available network services.

8.8. Static code analysis:

Security reviews of code stored in Humanity's source code repositories is performed, checking for coding best practices and identifiable software flaws.

8.9. Penetration testing:

Humanity maintains relationships with industry recognised penetration testing service providers for four annual penetration tests. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.

Limitations of Privilege & Authorisation Requirements

8.10. Service access:

A subset of Humanity's employees have access to the services and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Access is enabled through "just in time" requests for access; all such requests are logged. Employees are granted access by role, and reviews of high risk privilege grants are initiated daily. Employee roles are reviewed at least once every six months.

8.11. Background checks:

All Humanity employees undergo a third-party background check prior to being extended an employment offer, in accordance with the applicable laws. All employees are required to conduct themselves in a manner consistent with Humanity guidelines, non-disclosure requirements, and ethical standards.

Transmission Control

8.12. In-transit:

Humanity makes HTTPS encryption (also referred to as SSL or TLS) available on every one of its login interfaces. Humanity's HTTPS implementation uses industry standard algorithms and certificates.

8.13. At-rest:

Humanity stores user passwords following policies that follow industry standard practices for security. Humanity has implemented technologies to ensure that stored data is encrypted at rest when appropriate.

Input Control

8.14. Detection:

Humanity designed its infrastructure to log extensive information about the system behaviour, traffic received, system authentication, and other application requests. Internal systems aggregate log data and alert appropriate employees of malicious, unintended, or anomalous activities. Humanity personnel, including security, operations, and support personnel, are responsive to known incidents.

8.15. Response and tracking:

Humanity maintains a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, Humanity will take appropriate steps to minimise Customer damage or unauthorised disclosure.

8.16. Communication:

If Humanity becomes aware of unlawful access to Customer data stored within its services, Humanity will: 1) notify the affected Customers of the incident; 2) provide a description of the steps Humanity is taking to resolve the incident; and 3) provide status updates to the Customer contact, as Humanity deems necessary. Notification(s) of incidents, if any, will be delivered to one or more of the Customer's contacts in a form Humanity selects, which may include via email or telephone.

Availability Control

8.17. Infrastructure availability:

The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.95% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and HVAC services.

8.18. Fault tolerance:

Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer data is backed up to multiple durable data stores and replicated across multiple availability zones.

8.19. Online replicas and backups:

Where feasible, service databases are designed to replicate data between no less than 1 primary and 1 secondary database. All databases are backed up and maintained using at least industry standard methods.
Humanity's services are designed to ensure absolute customer satisfaction. The server instances that support the services are also architected with a goal to prevent support failure. This design assists Humanity operations in maintaining and updating the service applications and backend while limiting downtime.

9. International transfers

9.1. Adequacy

Humanity will provide an adequate level of protection for Personal Data that it processes on behalf of Customer in accordance with the requirements of EU Data Protection Legislation.

10. Service Data

10.1 Notwithstanding anything in this DPA, Humanity will have the right to collect, extract, compile, synthesize and analyze non-personally identifiable data or information resulting from Customer's use or operation of the Services ("Service Data") including, by way of example and without limitation, information relating to volumes, frequencies, recipients, bounce rates, or any other information regarding the communications Customer, its end users or recipients generate and send using the Services. To the extent any Service Data is collected or generated by Humanity, such data will be solely owned by Humanity and may be used by Humanity for any lawful business purpose without a duty of accounting to Customer or its recipients, provided that such data is used only in an aggregated form, without directly identifying any person. For the avoidance of doubt, this DPA will not apply to Service Data.

11. Miscellaneous

11.1. Except as amended by this DPA, the Agreement will remain in full force and effect.

11.2. If there is a conflict between the Agreement and this DPA, the terms of this DPA will control.

11.3. Any claims brought under this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement.

Customer Execution

Company legal name: ______________________________

Signed: ______________________________

Title: ____________________ Date: ______________

Humanity Execution

Humanity.com, Inc.

Signed: ______________________________

Title: ____________________ Date: ______________