DATA PROCESSING ADDENDUM

THIS DATA PROCESSING ADDENDUM ("Addendum") is incorporated into the System Inc. ("System") Enterprise Terms and Conditions of Use, Beta Terms of Use Agreement or, as applicable, the agreement between Customer and System (any of the foregoing the "Agreement") pursuant to which System agrees to provide the Service to Customer.

THE PARTIES AGREE THAT:

1. DEFINITIONS AND INTERPRETATION

1.1 In this Addendum (including the recitals above), the following terms shall have the meanings set out in this clause 1.1, unless expressly stated otherwise:

"**Addendum**"	means this Data Processing Addendum;
"**Agreement**"	means the Enterprise Terms and Conditions of Use, Beta Terms of Use Agreement or, as applicable, the agreement between Customer and System.
"**Anonymised Usage Data**"	means statistics concerning the use of the Service by Data Subjects which (a) has been anonymised and/or aggregated such that the Data Subject is not or is no longer identifiable (e.g. the number query runs per day per user) or (b) constitutes "aggregate consumer information" or has been "deidentified" (as such terms are defined in the CCPA);
"**CCPA**"	means the California Consumer Privacy Act of 2018 and any regulations promulgated thereunder, in each case, as amended from time to time;
"**Customer**"	means the person, corporation (including any non-profit corporation), general partnership, limited partnership, limited liability partnership, joint venture, estate, trust, company, firm or other enterprise, association or organization (including, without limitation, any governmental body or public entity) receiving the Service.
"**Customer Personal Data**"	means any Personal Data supplied by Customer for analysis using the Service that is Processed by System on behalf of Customer pursuant to or in connection with the Agreement;
"**Data Protection Laws**"	means all privacy and data protection laws, including the CCPA, and regulations, in each case, to the extent applicable to the Processing of Customer Personal Data;
"**Data Subject**"	means the identified or identifiable natural person to whom Personal Data relates;
"**Data Subject Request**"	means the exercise of rights by Data Subjects of Customer Personal Data under applicable Data Protection Laws;

"**Service**"	means those services and activities to be supplied to or carried out by or on behalf of System for Customer pursuant to the Agreement;
"**Personal Data**"	means (a) any information relating to an identified or identifiable natural person in connection with the Service and (b) any other information that constitutes personal information as defined in, and which is subject to, the CCPA. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that natural person.
"**Personal Data Breach**"	means a breach of System's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data in System's possession, custody or control. Personal Data Breaches do not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including, without limitation, unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems.
"**Process**" or "**Processing**"	means any operation or set of operations that is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
"**Subprocessor**"	means any third party appointed by or on behalf of System to Process Customer Personal Data; and

1.2 In this Addendum:

(a) unless otherwise defined herein, all capitalised terms shall have the meaning given to them in the Agreement;

(b) the singular includes the plural and vice versa, unless the context otherwise requires;

(c) references to this Addendum include its Schedules;

(d) references to clauses and/or Schedules are to clauses of, and Schedules to, this Addendum;

(e) the words "including" and "include" shall be construed only as illustration or emphasis and shall not be construed or take effect as limiting the generality of any earlier words;

(f) references to "laws" shall mean (a) any statute, regulation, by-law, or subordinate legislation; (b) the common law and the law of equity; (c) any

binding court order, judgment or decree; or (d) any industry code, policy or standard enforceable by law; and

1.3 This Addendum shall be incorporated into and form part of the Agreement. In the event of any conflict or inconsistency between this Addendum and the main body of the Agreement, this Addendum shall prevail.

2. PROCESSING OF CUSTOMER PERSONAL DATA

2.1 System shall:

(a) comply with Data Protection Laws as applicable to System in Processing Customer Personal Data; and

(b) not Process Customer Personal Data other than

(i) on Customer's instructions (subject always to clause 2.6);

(ii) as required by applicable laws; and

(iii) as necessary to perform its obligations and exercise its rights under the Agreement.

2.2 To the extent permitted by applicable laws, System shall inform Customer of:

(a) any Processing to be carried out under clause 2.1(b)(ii); and

(b) the relevant legal requirements that require it to carry out such Processing,

before the relevant Processing unless the relevant law prohibits System from doing so on important grounds of public interest.

1.1 Customer instructs System to Process Customer Personal Data only as necessary (i) to provide the Service to Customer (including, without limitation, to improve and update the Service, for security or business continuity purposes, troubleshooting and support, accounting purposes, and to carry out Processing initiated by Customer's authorized users (i.e., Team Members) and (ii) to perform System's obligations and exercise System's rights under the Agreement. System shall not retain, use or disclose any Customer Personal Data that constitutes "personal information" under the CCPA ("CA Personal Information") for any purpose other than for the specific purpose of providing the Service or as otherwise permitted by the CCPA, including by retaining, using, or disclosing the CA Personal Information for a commercial purpose (as defined in the CCPA) other than providing the Service. System shall not (i) sell any CA Personal information; (ii) retain, use or disclose any CA Personal Information outside of the direct business relationship between System and Customer. For purposes of CCPA, System hereby certifies that it understands the obligations under this Section 2.3 and will comply with them. Notwithstanding anything in the Agreement, this Addendum or any order form entered in connection therewith, the Parties acknowledge and agree that neither System's access to Customer Personal Data nor the exchange of Customer Personal Data between the Parties constitutes part of the consideration exchanged by the Parties in respect of the Agreement or any other business dealings.

2.3 Customer acknowledges and agrees that any instructions issued by Customer with regards to the Processing by System of Customer Personal Data pursuant to or in

connection with the Agreement shall (i) be strictly required for the sole purpose of ensuring compliance with Data Protection Laws, and (ii) not relate to the scope of the Service or otherwise materially change the services to be provided by System under the Agreement. Notwithstanding anything to the contrary herein, System may terminate the Agreement in its entirety upon written notice to Customer with immediate effect if System considers (in its absolute discretion) that (a) it is unable to adhere to, perform or implement any instructions issued by Customer due to the technical limitations of its systems, equipment and/or facilities, and/or (b) to adhere to, perform or implement any such instructions would require disproportionate effort (whether in terms of time, cost, available technology, manpower or otherwise).

2.4 Customer represents and warrants on an ongoing basis that there is, and will be throughout the term of the Agreement, a legal basis, to the extent required, under Data Protection Laws for the Processing by System of Customer Personal Data in accordance with this Addendum and the Agreement (including, without limitation, any and all instructions issued by Customer from time to time in respect of such Processing).

2.5 Customer acknowledges that System may create and derive Anonymised Usage Data from processing related to the Service, and use, publicise or share such Anonymized Usage Data with third parties to improve System's services and for its other legitimate business purposes.

3. SECURITY

3.1 System will implement and maintain technical and organizational measures designed to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access as described in Schedule 1 – Security Measures. System may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Service.

4. SUBPROCESSING

4.1 Customer generally authorizes System's engagement of any other third parties as Subprocessors ("Third Party Subprocessors").

4.2 Information about Subprocessors, including their functions and locations, is set forth in Schedule 2 – Authorized Subprocessors (as may be updated by System from time to time in accordance with this Addendum).

4.3 When engaging any Subprocessor, System will:

(a) ensure via a written contract that:

(i) the Subprocessor only accesses and uses Customer Personal Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the Agreement; and

4.4 When any new Third Party Subprocessor is engaged during the term of the Agreement, System will, at least thirty (30) days before the new Third Party Subprocessor Processes

any Customer Personal Data, notify Customer of the engagement (including the name and location of the relevant subprocessor and the activities it will perform).

4.5 Customer may object to any new Third Party Subprocessor by terminating its use of the Service or, as applicable, the Platform Agreement immediately upon written notice to System, on condition that Customer provides such notice within sixty (60) days of being informed of the engagement of the Third Party Subprocessor as described in clause 5.4. This termination right is Customer's sole and exclusive remedy if Customer objects to any new Third Party Subprocessor.

5. DATA SUBJECT RIGHTS

5.1 During the term of the Agreement, if System receives any request from a Data Subject in relation to Customer Personal Data, System will advise the Data Subject to submit its request to Customer and Customer will be responsible for responding to any such request. Taking into account the nature of the Processing, System shall, at Customer's cost, provide Customer with such assistance as may be reasonably necessary and technically possible in the circumstances, to assist Customer in fulfilling its obligation to respond to Data Subject Requests.

5.2 System shall:

(a) notify Customer if System receives a Data Subject Request; and

(b) not respond to any Data Subject Request except on the documented instructions of Customer (and in such circumstances, at Customer's cost) or as required by applicable laws, in which case System shall to the extent permitted by applicable laws inform Customer of that legal requirement before System responds to the Data Subject Request.

6. PERSONAL DATA BREACH

6.1 If System becomes aware of a Personal Data Breach, System will: (a) notify Customer of the Personal Data Breach without undue delay after becoming aware of the Personal Data Breach; and (b) promptly take reasonable steps to minimise harm and secure Customer Personal Data.

6.2 Notifications made pursuant to this clause will describe, to the extent possible and known, details of the Personal Data Breach, including steps taken to mitigate the potential risks and steps System recommends Customer take to address the Personal Data Breach.

6.3 Customer is solely responsible for complying with incident notification laws applicable to Customer and fulfilling any third party notification obligations related to any Personal Data Breach(s).

6.4 System's notification of or response to a Personal Data Breach under this clause 7 will not be construed as an acknowledgement by System of any fault or liability with respect to the Personal Data Breach

7. DELETION OR RETURN OF CUSTOMER PERSONAL DATA

7.1 Upon the expiration of the Subscription Period or earlier termination of the Agreement (the "Term End Date") subject to clause 7.2, Customer may in its absolute discretion by written notice to System within thirty (30) days of the Term End Date require System to

(a) return a complete copy of all Customer Personal Data to Customer by secure file transfer in such format as is reasonably notified by Customer to System; and/or (b) delete and all copies of Customer Personal Data Processed by System. System shall comply with any such written request as soon as reasonably practicable and in all events within ninety (90) days of the date Customer's written notice is received by System.

7.2 System may retain Customer Personal Data after the Term End Date to the extent required by applicable laws.

8. AUDIT RIGHTS

8.1 System will allow an independent auditor appointed by Customer to conduct audits (including inspections) to verify System's compliance with its obligations under this Addendum in accordance with clause 8. Provided, however, System may object in writing to an auditor appointed by Customer to conduct any audit if the auditor is, in System's reasonable opinion, not suitably qualified or independent, a competitor of System, or otherwise manifestly unsuitable. Any such objection by System will require Customer to appoint another auditor.

8.2 If the controls or measures to be assessed in the requested audit are addressed in an SOC 2 Type 2, ISO, NIST or similar audit report performed by a qualified third party auditor within twelve (12) months of Customer's audit request and System has certified in writing that there are no known material changes in the controls to be audited, Customer agrees to accept such report in lieu of requesting an audit of such controls or measures.

8.3 Prior to the commencement of any audit or inspection, System and Customer will discuss and agree in advance on: (i) the security and confidentiality controls applicable to any inspection or audit; and (ii) the reasonable start date, scope and duration of and security and confidentiality controls applicable to any audit.

8.4 Customer shall give System reasonable notice of any audit or inspection to be conducted under clause 8.1 (which shall in no event be less than thirty (30) days' notice unless required by a Supervisory Authority pursuant to clause 8.4(f)(ii)) and shall use its best efforts (and ensure that each of its mandated auditors uses its best efforts) to avoid causing, and hereby indemnifies System in respect of, any damage, injury or disruption to System's premises, equipment, personnel, data, and business (including any interference with the confidentiality or security of the data of System's other customers or the availability of the Service to such other customers) while its personnel are on those premises in the course of such an audit or inspection. Provided, however, that System need not give access to its premises, equipment, personnel, data, business, Security Documentation or systems for the purposes of such an audit or inspection:

(a) to any individual unless he or she produces reasonable evidence of identity and authority;

(b) to any auditor whom System has not given its prior written approval;

(c) unless the auditor enters into a non-disclosure agreement with System on terms acceptable to System;

(d) where, and to the extent that, System considers, acting reasonably, that to do so would result in interference with the confidentiality or security of the data of

System's other customers or the availability of the Service to such other customers;

(e) outside normal business hours at those premises; or

(f) on more than one (1) occasion in each period of twelve (12) months during the term of the Agreement (or where the term of the Agreement is less than twelve (12) months, on more than one (1) occasion during such shorter term), except for any additional audits or inspections which:

(i) Customer reasonably considers necessary because of a Personal Data Breach; or

(ii) Customer is required to carry out by Data Protection Law or a Supervisory Authority or other regulator, where Customer has identified the Personal Data Breach or the legal relevant requirement in its notice to System of the audit or inspection.

8.5 The Parties shall discuss and agree the costs of any inspection or audit to be carried out by or on behalf of Customer pursuant to this clause 8 in advance of such inspection or audit and, unless otherwise agreed in writing between the Parties, Customer shall bear any third party costs in connection with such inspection or audit and reimburse System for all costs incurred by System and time spent by System (at System's then-current professional services rates) in connection with any such inspection or audit.

9. TRANSFERS

9.1 System may store and Process Customer Personal Data anywhere System or its Subprocessors maintain facilities. System will provide information about the location of its data centers used to Process Customer Personal Data after receipt of a reasonable request.

SCHEDULE 1 – SECURITY MEASURES

System will implement and maintain the Security Measures set out in this Schedule 1. System reserves the right to revise the security measures set out in this Schedule 1 at any time, without notice, so long as such revisions do not materially reduce the protection provided for Personal Data that System processes in the course of providing the Service.

1) Organizational management and staff responsible for the development, implementation and maintenance of System's information security controls. Executive leadership is involved in reviewing and approving all security policies.

2) Audit and risk assessment procedures for the purposes of periodic review and assessment of security risks to System's organization, monitoring compliance with System's policies and procedures, and reporting the condition of its information security and compliance to internal senior management.

3) Data security controls that include logical segregation of data, restricted (e.g. role-based) access and monitoring, and utilization of commercially available and industry standard encryption technologies for Personal Data.

a) Encryption in Transit: Customer content is encrypted in transit using Transport Layer Security. TLS is active on all accounts by default and cannot be disabled by end users.

b) Encryption at Rest: Confidential customer data is encrypted at rest with Advance Encryption Standard (AES). Backups are encrypted at rest.

4) Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions. Access accounts are provisioned for engineers on their hire date and deprovisioned on their closing date by a member of the senior engineering staff.

5) User IDs and password configuration requirements have been established that are designed to prevent unauthorized access to production systems. System has defined the following password requirements: (i) password length must have a minimum of 10 characters; (ii) password must contain both upper and lowercase characters; (iii) password must contain a number (0-9) and/or a special character; (iv) Password must be different from user's previous 10 passwords; and (v) password must be changed annually.

6) With respect to physical and environmental security, System's production resources are hosted in Amazon Web Services. Physical and environmental security is handled entirely by Amazon and their vendors. Amazon has provided a list of compliance and regulatory security assurances, including representations of SOC 1-3, and ISO27001 compliance.

7) Operational procedures and controls to provide for application deployment and change management, capacity management, and separation of development, testing and production.

8) Incidents are handled in accordance with System's Incident Response Plan following the lifecycle of an incident: Discovery, Acknowledgement, Verification, Scope, Resolution and finally Response. The Privacy Officer(s) and Director of Engineering are responsible for managing the

response process in accordance with the IRP, completing an after-action review and coordinating any outbound communication that may be necessary following an incident.

9) Network security controls designed and implemented so that internet connections are required to use transport encryption. Default deny has been established for each application/service group/layer. Service to service connections must be explicitly allowed.

10) Vulnerability assessment and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.

11) Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergency situations or disasters.

SCHEDULE 2 – AUTHORIZED SUBPROCESSORS

Name	Function	Location
Amazon Web Services	Data storage and processing	AWS servers located in the United States only
Terraform Cloud	Infrastructure Management	Terraform servers located in the United States only
Google Analytics	Customer Analytics	Google servers located in the United States only
Segment	Data Processing	Segment servers located in the United States only