DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is made part of and incorporated into the Master Software License and Services Agreement, or any other written agreement, between the applicable Quorum entity ("**Quorum**") and Customer ("**Agreement**"), each as identified in the Agreement, for software subscription or other services ("**Services**"). This DPA is effective as of the date of the Effective Date of the Agreement.

1. **Definitions**. Unless specified herein the capitalized terms in this DPA shall bear the meaning of ascribed in the Agreement. For the purposes of this DPA, the definitions are as follows:

a. "**Applicable Data Protection Laws**" means all laws and binding regulations, including but not limited to the laws and regulations of the European Economic Area and its Member States, Switzerland, the United Kingdom, and the United States, including federal and state laws in California and other states, applicable to the Processing of Personal Data under the Agreement;

b. "**Controller**" means the natural or legal person or organization who determines the purposes and means of the processing of Personal Data;

c. "**Data Exporter**" means the entity who provides Personal Data and Processing instructions to the Processor or Subprocessor for Processing on behalf of the Data Exporter;

d. "**Data Importer**" means the Processor, Subprocessor who agrees to receive from the Data Exporter Personal Data intended for Processing on the Data Exporter's behalf after the transfer in accordance with the Data Exporter's instructions;

e. "**Data Subject**" means the identified or identifiable person to whom Personal Data relates;

f. "**Data Subject Request**" means a communication from a Data Subject regarding the exercise of rights regarding their Personal Data pursuant to Applicable Data Protection Law;

g. "**Documented Instructions**" means all instructions from the Controller to Quorum in connection with the Services regarding the Processing or Transfer of Personal Data, including without limitation the terms of this DPA (including Schedule A), instructions submitted through or implemented on any forum or portal made available to Customer in connection with the Services, and any other written agreement entered into between Customer and Quorum;

h. "**Personal Data**" means information that (a) constitutes personal data, personal information, or a similar term under Applicable Data Protection Laws, or (b) can be used directly or indirectly, alone or in combination with other information, to identify a natural living person, and, in each case of (a) and (b), is Processed by Quorum as a Processor, on behalf of Customer as the Controller, under the Agreement;

i. "**Personal Data Breach**" means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by Quorum in connection with the Services under the Agreement;

j. "**Process**" (or inflections thereof) means any operation, or set of operations, which 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;

k. "**Processing Specification Form**" or "**PSF**" means the document appended to an Order bearing this title, which describes the Personal Data Processing activities in connection with the Services;

l. "**Processor**" means an entity that processes Personal Data on behalf of, and in accordance with, the instructions of a Controller. "Processor" shall include "service provider" as defined by Applicable Data Protection Laws;

m. "**Subprocessor**" means the entity Processing Personal Data on behalf of the Processor;

n. "**Transfer**" means to disclose or otherwise make Personal Data available to a third party (including to any affiliate), either by physical movement of the Personal Data to a third party or by enabling access to the Personal Data by other means; and

o. "**Transfer Clauses**" means the relevant module of the Standard Contractual Clauses for approved by European Union Commission Decision of 4 June 2021, which are incorporated herein by reference and as supplemented by Schedule C, as applicable.

2. **Relationship of the Parties**. The Parties agree that, with respect to the Processing of Personal Data within the provision of the Services, Customer is the Controller and Quorum is the Processor.

3. **Scope and Operation**.

a. The details of Processing are set forth in Schedule A of this DPA. The Parties acknowledge and agree that where a PSF is appended to an Order, the PSF is incorporated herein by reference as Schedule A in place of the Schedule A attached to this DPA, and shall be deemed "Annex 1" for purposes of the Transfer Clauses.

b. This DPA shall apply until the later of (i) the term of the Agreement, or (ii) Quorum has returned or deleted all Personal Data in accordance with the Agreement.

4. **Subprocessors**.

a. Customer acknowledges and agrees that Quorum is permitted to engage Subprocessors in the provision of Services. Customer consents to Quorum's use of the Sub-processors listed in any applicable PSF;

b. Customer may obtain a current list of Subprocessors, and/or subscribe to receive notifications regarding changes to the list of Subprocessors, using the weblink provided in the applicable PSF, or where there is no applicable PSF, by contacting Quorum at dpp@quorumsoftware.com;

c. To the extent required by Applicable Data Protection Law, Quorum shall provide Customer with notification of a new Subprocessor at least thirty (30) days before authorizing such Subprocessor to Process Personal Data. Customer may reasonably object to Quorum's use of a new Subprocessor by notifying Quorum in writing within fifteen (15) days after receipt of such notice, provided that Customer's objection shall include a detailed explanation of the grounds for objection and a proposal to reasonably resolve the objection;

d. Following an objection raised under clause 4(c), Quorum shall take commercially reasonable measures to implement an agreeable alternative to the objected-to Subprocessor. Where the Parties in good faith cannot agree on any alternative by the end of the notice period contemplated in clause (c) above, Customer may terminate the affected portion of the Services, in accordance with any right to terminate for convenience under the Agreement; and

e. Subprocessors engaged by Quorum shall be bound by a written agreement requiring the Subprocessor to adhere, in substance, to data protection obligations no less stringent than those applicable to Quorum under this DPA. Quorum shall remain fully liable to Customer for the performance of Subprocessors' obligations under this DPA.

5. **Processing of Personal Data**. The following terms apply to Quorum's processing of Personal Data for purposes of providing Services pursuant to the Agreement:

   a. Quorum shall process Personal Data only (i) as necessary to provide the Services; (ii) in accordance with the Documented Instructions; and (iii) as necessary to comply with applicable law (and Quorum will provide prior notice to Customer of any such legal obligations that are outside of the Documented Instructions, unless that law prohibits such disclosure);

   b. Quorum shall promptly notify Customer of any Documented Instruction that, in Quorum's opinion, infringes on any Applicable Data Protection Law; provided, however, that Customer is responsible for ensuring that the Documented Instructions comply with Applicable Data Protection Laws; and

   c. Notwithstanding the limitations in clause 5(a), Quorum may, to the extent consistent with Quorum's role as a Processor, Process Personal Data as necessary to (i) retain and employ Subprocessors, subject to the requirements in Section 4, (ii) build or improve Quorum's products and services, provided such Processing does not include building or modifying data Subject profiles that will be used to provide services to another customer or to correct or augment data acquired from another source, (iii) detect, prevent, and investigate data security incidents that may impact Personal Data or systems Processing Personal Data, (iv) detect, prevent, and investigate fraudulent or illegal activity, and (v) create System Data (as defined in the Agreement) and use such System Data for the purposes of (i)-(iv).

6. **Security of Personal Data**. Quorum shall implement and maintain technical and organizational measures to safeguard Personal Data appropriately appropriate to the risks presented by the Processing and the nature of the Personal Data to be protected. Such safeguards are set forth in Schedule B;

7. **Assistance to Customer**. Taking into account the nature of Processing performed under the Agreement and the information available to Quorum, Quorum shall assist Customer for the fulfillment of Customer's obligations under Applicable Data Protection Laws, including regarding data protection impact assessments, communication of Personal Data Breaches to Data Subjects, security of Personal Data, and consultation with or notifications to governmental authorities. Customer shall make a written request for any assistance under this Section. Quorum may invoice Customer for any documented, direct, reasonable costs (based on standard hourly rates for professional services) resulting from its efforts to provide any such assistance.

8. **Data Subject Requests**. If Quorum receives a Data Subject Request, Quorum shall:

   a. promptly and without undue delay notify Customer of the Data Subject Request;

   b. respond to the Data Subject solely to indicate that the Data Subject must contact the applicable controller, and identifying Customer if reasonably feasible;

   c. not otherwise respond to the Data Subject Request except as contemplated by the foregoing clause (ii); and

   d. reasonably assist Customer by appropriate technical and organizational measures, insofar as this is reasonably feasible, for the fulfilment of Customer's obligation to respond to Data Subject Requests in accordance with Applicable Data Protection Laws.

9. **Audits**. Quorum shall provide all information reasonably necessary to demonstrate compliance with Applicable Data Protection Laws, including to allow for and contribute to audits in accordance with Applicable Data Protection Laws, including inspections by Customer of Quorum's performance of its Processing obligations under this DPA, provided that:

   a. Customer or person undertaking the audit on behalf of Customer shall give at least thirty (30) days' prior written notice to Quorum (including notice of the requested scope and means of the audit) and shall use all reasonable efforts to avoid and minimize any damage, injury or disruption to Quorum's premises, equipment, personnel, and business;

b. Any third party appointed by Customer to conduct any audit shall be suitable, reasonably qualified, and independent. Customer shall bind any such auditor to a duty of confidentiality, which may include, at Quorum's request, entering a confidentiality and non-disclosure agreement between any of the auditor, Customer, and/or Quorum, at Quorum's request;

c. Quorum shall not, unless strictly required by law, be required to provide (i) access to its premises; (ii) any information to any individual without reasonable evidence of that individual's identity and authority; (iii) access or information outside normal business hours; or (iv) assistance in relation to more than one (1) audit in any calendar year, unless an additional audit is required by applicable law or is reasonable in light of material and genuine concerns as to Quorum's compliance with the DPA; and

d. The Parties agree that Quorum may satisfy any audit request by producing a written report, or summary or redacted version thereof, generated by a reputable third-party auditor, that evidences Quorum's adherence to SSAE 18 standards, provided, however, that such report shall be Quorum's confidential information, and provided that nothing in this clause (c) varies, modifies, or affects any rights of governmental authorities or Data Subjects under Applicable Data Protection Law;

e. Quorum shall reasonably assist with any additional right of Customer to audit or inspect Quorum's compliance with this DPA or Applicable Data Protection Law as conferred on Customer by Applicable Data Protection Law; and

f. Customer shall bear all costs of an audit or inspection; however, if the audit reveals material deficiencies in Quorum's performance under this DPA, each Party shall bear its own costs of that audit or inspection.

10. International Transfers.

a. The Parties shall comply with all applicable Data Protection Law regarding any cross-border transfer of Personal Information, including without limitation the provisions of Schedule C to this DPA, to the extent required by Applicable Data Protection Law in connection with the Processing or Transfer of Personal Data under the Agreement;

b. In the event of any changes in Applicable Data Protection Law, such as the Transfer Clauses in Schedule C being amended, replaced, or repealed by the European Commission, the United Kingdom, or under Applicable Data Protection Law, the Parties shall work together in good faith to enter into an updated version of the Transfer Clauses (to the extent required) or other approved transfer mechanism, or negotiate in good faith a solution to enable a transfer of Personal Data to be conducted in compliance with Applicable Data Protection Law; and

c. Customer agrees that Quorum may transfer Personal Data to Subprocessors, including third parties established in other jurisdictions, provided that such transfers comply with Applicable Data Protection Law and the provisions of this DPA, including but not limited to onward transfer provisions set forth in the Transfer Clauses.

11. Personal Data Breach.

a. Quorum shall notify Customer without undue delay, and in any event within seventy-two (72) hours after becoming aware of a Personal Data Breach involving Personal Data Processed in association with Quorum's provision of Services under the Agreement. Such notification shall include, to the extent known, a description of the nature and extent of the Personal Data Breach, categories and numbers of affected Data Subjects and Personal Data records, and the measures taken or proposed to be taken to address the Personal Data Breach, with updates provided to Customer as new information becomes available;

b. Quorum shall promptly investigate and take appropriate steps to remediate a Personal Data Breach;

c. Quorum shall take all commercially reasonable measures to mitigate the affect on Data Subjects, taking into account the nature of the Personal Data and risks to such data;

d. Quorum shall not release or publish any filing, communication, notice, press release, or report, or communicate directly with affected Data Subjects concerning the Personal Data Breach in a manner that identifies Customer or its affected Data Subjects without Customer's prior written approval, unless Quorum is required to do so by Applicable Data Protection Laws;

e. Customer shall not release or publish any filing, communication, notice, press release, or report, or communicate directly with affected Data Subjects concerning the Personal Data Breach in a manner that identifies Quorum without Quorum's prior written approval, unless Customer is required to do so by Applicable Data Protection Laws; and

f. Where the Personal Data Breach was caused by Quorum's failure to comply with this DPA or Applicable Data Protection Law regarding the safeguarding or security of Personal Data, Quorum shall reimburse Customer for the reasonable, documented costs incurred directly by Customer in notifying affected Data Subjects to the extent required by Applicable Data Protection Law.

g. In no event will Quorum be liable for any Personal Data Breach that arises from Customer's actions, negligence, or misconduct, including Customer instructions, Customer employees' or contractors' failure to maintain reasonable password security, theft or loss of a Customer device, or Customer permitting a third party to access Personal Data.

12. **Confidentiality**. Quorum shall ensure that persons authorized to Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Quorum shall take steps to limit access to Personal Data to Quorum's personnel and Subprocessors who require such access in order to perform the Services.

13. **Deletion or Return of Personal Data.** Quorum shall, within fifteen (15) business days of receipt of Customer's written request, permanently delete or securely return all Personal Data Processed on behalf of Customer to Customer after termination of the Agreement unless otherwise required by law, except that Quorum will delete Personal Data contained on backups and in archives in the normal course of business according to Quorum's standard deletion times so long as such Personal Data is not subject to active Processing activities.

14. **Compliance with Law**.

a. The Parties agree to comply with Applicable Data Protection Laws with respect to the Processing of Personal Data in association with the Agreement. To the extent applicable, the Parties agree to comply with the jurisdiction-specific provisions set forth in Schedule C; and

b. Customer shall have sole responsibility for the accuracy, quality and legality of Personal Data and the means by which Customer acquires it. Quorum shall have no obligation to assess the contents of the Personal Data to identify information subject to any specific legal requirements.

15. **Costs.** Unless otherwise expressly stated herein, Quorum shall have the right to invoice any documented, direct, and reasonable costs (based on hourly internal rates) resulting from its efforts to assist Customer with Customer's obligations, or comply with Customer's additional instructions beyond the Documented Instructions, including under Sections 7, 8, and 9 (except Section 9(d)) of this DPA.

16. **Precedence**. This DPA is hereby incorporated by reference into the Agreement. The parties do not intend that anything in this DPA will be construed to cancel or negate any obligation in the Agreement. Additionally:

a. To the extent any term in the Agreement conflicts with this DPA, this DPA will control;

b. To the extent any term in the Transfer Clauses conflicts with this DPA, the Transfer Clauses will control; and

c. To the extent any term of the Agreement (including the DPA or Transfer Clauses) conflicts with any applicable term in Schedule C, the applicable term in Schedule C shall control.

SCHEDULE A: Description of Processing

ANNEX I

This Annex I describes the Processing of Personal Data within the Services.

LIST OF PARTIES

Data exporter(s):

The name, address, contact details, signature, and date of execution for Data Exporter shall be that of Quorum under the Agreement for purposes of P-to-C Transfer Clauses, and that of Customer under the Agreement for purposes of the C-to-P Transfer Clauses.

Activities relevant to the data transferred under these Clauses: Quorum's provision, and Customer's use, of the Services

Role: Controller (for purposes of C-to-P Transfer Clauses) / Processor (for purposes of P-to-C Transfer Clauses

Data importer(s):

The name, address, contact details, signature, and date of execution for Data Importer shall be that of Customer under the Agreement for purposes of P-to-C Transfer Clauses, and that of Quorum under the Agreement for purposes of the C-to-P Transfer Clauses..

Activities relevant to the data transferred under these Clauses: Quorum's provision, and Customer's use, of the Services

Role: Controller (for purposes of P-to-C Transfer Clauses) / Processor (for purposes of C-to-P Transfer Clauses

A. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- Customer's Users (including personnel or agents of Customer)
- Customer's suppliers, customers, and clients

Categories of personal data transferred

- Login credentials
- Usage data, including IP address, device identifiers, and data regarding use of the Services
- Contact information input into and Processed within the Services, including name, title, address, telephone number, email address, and employer
- Government-issued identification number
- Employment/HR information, including career history, recruitment and termination details, employee assessments, and training and security records
- Geolocation data
- Information technology management details, including logs and journal tables related to incident tickets and service requests made by Customer and its Users

Sensitive data transferred (if applicable) 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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None

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

Continuous

Nature of the processing

As necessary to provide the Services or otherwise permitted by the Agreement

Purpose(s) of the data transfer and further processing

Quorum shall Process Personal Data as necessary to perform the Services pursuant to the Agreement, in accordance with the Documented Instructions.

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

Duration of the Agreement, unless otherwise agreed in writing.

B. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The competent supervisory authority shall be the supervisory authority which is competent to supervise the activities of the Data Exporter.

SCHEDULE B

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

Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons, available at: Technical and Organizational Measures for Data Protection

SCHEDULE C

JURISDICTION-SPECIFIC CLAUSES

I. Australia

A. The following provisions apply to all transfers and Processing of Personal Data controlled by Data Exporter in Australia.

B. For the avoidance of doubt, "Applicable Data Protection Laws" includes the Australian Privacy Act 1988 (Cth), as amended from time to time, including the Australian Privacy Principles or any equivalent privacy principles that take their place.

C. When Processing Personal Data, Quorum will comply with Applicable Data Protection Laws, including the Australian Privacy Principles.

II. European Economic Area

A. For the purposes of this Section:

(a) "**EU**" means the European Economic Area;

(b) "**EU Data Protection Laws**" means any applicable laws of Europe that relate to the Processing of Personal Data under this Agreement.

(c) "**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016.

B. To the extent that any Data Exporter transfers Personal Data subject to EU Data Protection Laws, either directly or via onward transfer, to a Data Importer located in a country that does not ensure an adequate level of protection within the meaning of EU Data Protection Laws, the Parties agree to comply with the terms of the Transfer Clauses in accordance with the following:

(a) if the Data Importer acts as a Processor of that Personal Data, the Data Exporter and Data Importer shall comply with the terms of the C-to-P Transfer Clauses, which are hereby incorporated into this Agreement by reference; or

(b) if the Data Exporter is the Processor of Personal Data to be exported and the Data Importer determines the purposes and means of the Processing of the Personal Data but the Data Importer's Processing is not otherwise subject to European Data Protection Laws, the Data Exporter and Data Importer shall comply with the terms of the P-to-C Transfer Clauses, which are hereby incorporated into this Agreement by reference.

C. For the purposes of the C-to-P Transfer Clauses, the following additional provisions shall apply:

(a) the names and addresses of those Data Exporter(s) and Data Importer(s) shall be considered to be incorporated into the Transfer Clauses;

(b) The Parties' signature to this Agreement shall be considered as signature to the Transfer Clauses;

(c) Clause 7 (Docking Clause) shall apply;

(d) Option 2 under paragraph (a) of Clause 9 (Use of subprocessors) shall apply and "[Specify time period]" be replaced with "thirty (30) days" (This subsection (d) only applies to the C-to-P Transfer Clauses, and not to the P-to-C Transfer Clauses);

(e) The option under Clause 11 (Redress) shall not apply;

(f) For the purposes of paragraph (a) of Clause 13 (Supervision), the Data Exporter shall be considered as established in an EU Member State (This subsection (d) only applies to the C-to-P Transfer Clauses, and not to the P-to-C Transfer Clauses);

(g) The governing law for the purposes of Clause 17 (Governing law) shall be the law of the Norway;

(h) The courts under Clause 18 (Choice of forum and jurisdiction) shall be the courts of Norway;

(i) The contents of Schedule A, as applicable, shall form Annex I to the Transfer Clauses;

(j) The supervisory authority competent to supervise the activities of Data Exporter shall act as competent Supervisory Authority for the purposes of Annex I.C of the Transfer Clauses;

(k) The contents of Schedule B shall form Annex II of the Transfer Clauses (Technical and organisational measures including technical and organisational measures to ensure the security of the data).

III. Malaysia

A. For the avoidance of doubt, "Applicable Data Protection Laws" includes the Malaysian Personal Data Protection Act 2010, which shall include implementing measures to comply with obligations prescribed by the Malaysian Personal Data Protection Commissioner from time to time, including the Personal Data Protection Standards 2015, as may be amended or supplemented from time to time.

IV. Switzerland

A. For the purposes of this Section, the term "**Swiss Data Protection Laws**" means Switzerland's Federal Act on Data Protection of June 19, 1992, the Ordinance to the Federal Act on Data Protection, and the Ordinance on Data Protection Certification, and all Swiss laws relating to the Processing, privacy, protection, or use of Personal Data.

B. To the extent any Data Exporter Transfers Personal Data subject to Swiss Data Protection Laws, either directly or via onward transfer, to a Data Importer located in a country that does not ensure an adequate level of protection within the meaning of Swiss Data Protection Laws, the Parties agree to the Transfer Clauses in accordance with the following clauses C of this Section.

C. The following additional provisions shall apply so that the Transfer Clauses are suitable for providing an adequate level of protection for such transfer under Swiss Data Protection Laws:

(a) "**FDPIC**" means the Swiss Federal Data Protection and Information Commissioner;

(b) "**Revised FADP**" means the revised version of the Federal Act of Data Protection ("**FADP**") of 25 September 2020;

(c) The term "**EU Member State**" must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility for suing their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c);

(d) The Transfer Clauses also protect the data of legal entities until the entry into force of the Revised FADP;

(e) The FDPIC shall act as the "competent Supervisory Authority" insofar as the relevant data transfer is governed by the FADP.

V. United Kingdom

A. For the purposes of this Section:

(a) "**UK**" means the United Kingdom;

(b) "**UK Data Protection Laws**" means the UK GDPR, Data Protection Act of 2018, and all UK laws relating to the Processing, privacy, protection, or use of Personal Data;

(c) "**UK GDPR**" means the United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

B. To the extent any Data Exporter Transfers Personal Data subject to UK Data Protection Laws, either directly or via onward transfer, to a Data Importer located in a country that does not ensure an adequate level of protection within the meaning of UK Data Protection Laws, the Parties agree to the Transfer Clauses in accordance with the following clause C of this Section.

C. The following additional provisions shall apply so that the Transfer Clauses are suitable for providing an adequate level of protection for such transfer under UK Data Protection Laws:

(a) Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 28 January 2022, as it is revised under Section 18 of those Mandatory Clauses, shall apply;

(b) The information required by Part 1, Tables 1 to 3 of the Approved Addendum is set out in Schedules A and B.

(c) With respect to Section 19 of the Approved Addendum, in the event the Approved Addendum changes, neither Party may end the Addendum except as provided for in the Agreement.

VI. United States

The following provisions apply to the provision of Personal Data from one Party (the "**Disclosing Party**") to another Party (the "**Recipient**") that is subject to the laws of any state of the United States ("**US Personal Data**"), including without limitation the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020 ("**CCPA**") , Colorado Privacy Act, Col. Rev. Stat. § 6-1-1301 et seq., Connecticut Data Privacy Act, S.B. 6, Virginia, or Utah Consumer Privacy Act, S.B. 227, each as amended or supplemented from time to time ("**US Data Protection Law**").

A. To the extent the Disclosing Party discloses Deidentified data (as that term is defined in US Data Protection Law) derived from US Personal Data to Recipient, or to the extent Recipient creates Deidentified data from US Personal Data received from or on behalf of the Disclosing Party, Recipient shall:

(a) adopt reasonable measures to prevent such Deidentified data from being used to infer information about, or otherwise being associated with, a particular natural person or, where required by US Data Protection Law, a household;

(b) publicly commit to maintain and use such Deidentified data in a deidentified form and to not attempt to re-identify the Deidentified data, except that Recipient may attempt to re-identify the data solely for the purpose of determining whether its deidentification processes satisfy the requirements of US Data Protection Law, as applicable; and

(c) contractually obligate any recipients of the Deidentified data, including sub-processors, contractors, and other third parties, to comply with the provisions of this Section.

B. Where the Disclosing Party acts as a Business with respect to US Personal Data subject to the CCPA ("**California Personal Data**") and Recipient acts as a Service Provider of such US Personal Data (as the terms "Business" and "Service Provider" are defined under CCPA):

(a) Recipient agrees that it Processes California Personal Data as a Service Provider when providing the Services;

(b) Recipient acknowledges that the Disclosing Party is disclosing California Personal Data in connection with the Agreement only for the limited and specific purposes of receiving the Services;

(c) Recipient shall (a) retain, use, disclose, or otherwise process California Personal Data solely on behalf of the Disclosing Party for the specific purpose of providing the Services or as otherwise required by law; (b) Process California Personal Data at all times in compliance with the CCPA and the Agreement; and (3) provide the same level of privacy protection as is required by the CCPA;

(d) Recipient shall not: (a) retain, use, disclose, or otherwise process California Personal Data except as necessary to provide the Services or as otherwise required by law; (b) sell or share California Personal Information (as "sell" and "share" are defined under the CCPA); (c) Process California Personal Data in any manner outside of the direct business relationship between Disclosing Party and Recipient; or (d) combine any California Personal Data with Personal Data that it receives from or on behalf of any other third party or its interactions with "consumers" (as defined under the CCPA), provided that Recipient may so combine California Personal Information for a "business purpose" (as defined under the CCPA) if directed to do so by the Disclosing Party or as otherwise expressly permitted by the CCPA;

(e) Recipient agrees to cooperate with any reasonable and appropriate audits, inspections, or other steps that the Disclosing Party deems reasonably necessary to confirm that Recipient processes California Personal Data in a manner consistent with the Disclosing Party's obligations under the CCPA;

(f) Disclosing Party may, upon reasonable notice to Recipient, take all reasonable and appropriate steps to prevent, stop, or remediate any unauthorized processing of California Personal Data; and

(g) Recipient agrees to immediately notify Disclosing Party in writing if it can no longer comply with the CCPA or its obligations under this Agreement.