DATA PROCESSING ADDENDUM

The customer ("Customer") and ColdQuanta, Inc. ("ColdQuanta") enter into this Data Processing Addendum (including the annexes attached hereto, this "DPA") and it is incorporated into and forms part of the ColdQuanta Terms of Use (as amended, the "Agreement") between the parties.

1. Definitions

For purposes of this DPA, the terms below have the meanings set forth below. Capitalized terms that are used but not defined in this DPA have the meanings given in the Agreement.

(a) Affiliate means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity, where "control" refers to the power to direct or cause the direction of the subject entity, whether through ownership of voting securities, by contract or otherwise.

(b) Applicable Data Protection Laws means European Data Protection Laws and the CCPA, in each case, to the extent applicable to the relevant Personal Data or Processing thereof under the Agreement.

(c) CCPA means the California Consumer Privacy Act of 2018 and any binding regulations promulgated thereunder.

(d) Customer means the person that enters into the Cold Quant Terms of Use.

(e) Customer Data means information provided or made available to ColdQuanta for Processing on Customer's behalf to perform the Services.

(f) EEA means the European Economic Area.

(g) European Data Protection Laws means the GDPR and other data protection laws of the European Union, its Member States, Switzerland, Iceland, Liechtenstein, Norway and the United Kingdom, in each case, to the extent applicable to the Processing of Personal Data under the Agreement.

(h) GDPR means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, as amended from time to time.

(i) Information Security Incident means a breach of ColdQuanta's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data in ColdQuanta's possession, custody or control. Information Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks or other network attacks on firewalls or networked systems.

(j) Personal Data means Customer Data that constitutes "personal data," "personal information," or similar information governed by Applicable Data Protection Laws, except that Personal Data does not include such information pertaining to Customer's business contacts who are Customer personnel where ColdQuanta acts as a controller of such information.

(k) Processing means any operation or set of operations which is performed on Personal Data or on sets of personal data, whether or not by automated 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.

(l) Security Measures has the meaning given in Section 4(a) (ColdQuanta's Security Measures).

(m) Standard Contractual Clauses means the mandatory provisions of the standard contractual clauses for the transfer of personal data to processors established in third countries in the form set out by European Commission Decision 2010/87/EU.

(n) Subprocessors means third parties that ColdQuanta engages to Process Personal Data in relation to the Service.

(o) Third Party Subprocessors has the meaning given in Section 5 (Subprocessors) of Annex 1.

(p) The terms controller, data subject, processor and supervisory authority as used in this DPA have the meanings given in the GDPR.

2. Duration and Scope of DPA

(a) This DPA will remain in effect so long as ColdQuanta Processes Personal Data, notwithstanding the expiration or termination of the Agreement.

(b) Annex 1 (EU Annex) to this DPA applies only to the Processing of Personal Data subject to European Data Protection Laws. Annex 2 (California Annex) to this DPA applies only to the Processing of Personal Data subject to the CCPA with respect to which Customer is a Business (as defined in the CCPA).

3. Customer Instructions

ColdQuanta will Process Personal Data only in accordance with Customer's instructions. By entering into this DPA, Customer instructs ColdQuanta to Process Personal Data to provide the Service and to perform its other obligations and exercise its rights under the Agreement, including without limitation to (i) carry out the Service or the business of which the Service is a part; (ii) carry out any benefits, rights and obligations relating to the Service; (iii) maintain records relating to the Service; or (iv) comply with any legal or self-regulatory obligations relating to the Service. Customer acknowledges and agrees that ColdQuanta may create and derive from Processing related to the Service, anonymized and/or aggregated data that does not identify Customer or any natural person and use, publicize, or share with third parties such data to improve ColdQuanta's products and services and for its other legitimate business purposes.

4. Security

(a) ColdQuanta Security Measures. ColdQuanta will implement and maintain administrative, technical, physical and organizational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration or unauthorized disclosure of or acquisition to Personal Data (the "Security Measures") as described in Annex 3 (Security Measures). ColdQuanta may update the Security Measures from time to time, provided the updated measures do not decrease the overall protection of Personal Data.

(b) Information Security Incidents. ColdQuanta will notify Customer without undue delay of any Information Security Incident affecting Personal Data of which Customer becomes aware. Such notifications will describe available details of the Information Security Incident, including steps taken to mitigate the potential risks and steps ColdQuanta recommends Customer take to address the Information Security Incident. ColdQuanta's notification of or response to an Information Security Incident will not be construed as ColdQuanta's acknowledgement of any fault or liability with respect to the Information Security Incident.

(c) Customer's Security Responsibilities and Assessment

(i) Customer's Security Responsibilities. Customer agrees that, without limitation of ColdQuanta's obligations under Section 4 (Security), Customer is solely responsible for its use of the Service, including (a) making appropriate use of the Service to ensure a level of security appropriate to the risk in respect of the Personal Data; (b) securing the account authentication credentials, systems and devices Customer uses to access the Service; (c) securing Customer's systems and devices that ColdQuanta uses to provide the Service; and (d) backing up Personal Data.

(ii) Customer's Security Assessment. Customer agrees that the Service, the Security Measures and ColdQuanta's commitments under this DPA are adequate to meet Customer's needs, including with respect to any security obligations of Customer under Applicable Data Protection Laws, and provide a level of security appropriate to the risk in respect of the Personal Data.

5. Data Subject Rights

(a) ColdQuanta's Data Subject Request Assistance. ColdQuanta will (taking into account the nature of the Processing of Personal Data) provide Customer with assistance reasonably necessary for Customer to perform its obligation under Applicable Data Protection Laws to fulfill requests by data subjects to exercise their rights under Applicable Data Protection Laws ("Data Subject Requests") with respect to Personal Data in ColdQuanta's possession or control. Customer shall compensate ColdQuanta for any such assistance at ColdQuanta's then-current professional services rates, which shall be made available to Customer upon request.

(b) Customer's Responsibility for Requests. If ColdQuanta receives a Data Subject Request, ColdQuanta will advise the data subject to submit the request to Customer and Customer will be responsible for responding to any such request.

6. Customer Responsibilities

Customer represents and warrants to ColdQuanta that Customer Data does not and will not contain any social security numbers or other government-issued identification numbers, protected health information subject to the Health Insurance Portability and Accountability Act (HIPAA) or other information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; health insurance information; biometric information; passwords to any online accounts; credentials to any financial accounts; tax return data; any payment card information subject to the Payment Card Industry Data Security Standard; personal data of children under 13 years of age; or any other information that falls within any special categories of data (as defined in GDPR).

7. Miscellaneous

(a) Liability Cap. The total combined liability of either party and its Affiliates towards the other party and its Affiliates, whether in contract, tort or any other theory of liability, under or in connection with Agreement, this DPA and the Standard Contractual Clauses if entered into as described in Annex 1, Section 4 (Transfers out of the EEA) combined will be limited to limitations on liability or other liability caps agreed to by the parties in the Agreement, subject to Section 7(b) (Liability Cap Exclusions).

(b) Liability Cap Exclusions. Nothing in Section 7(a) (Liability Cap) will affect any party's liability to data subjects under the third party beneficiary provisions of the Standard Contractual Clauses to the extent limitation of such rights is prohibited by European Data Protection Laws, where applicable.

(c) Conflict. Except as expressly modified by the DPA, the terms of the Agreement remain in full force and effect. To the extent of any conflict or inconsistency between this DPA and the other terms of the Agreement, this DPA will govern.

(d) General. Notwithstanding anything in the Agreement or any order form entered in connection therewith to the contrary, the parties acknowledge and agree that ColdQuanta's access to Personal Data does not constitute part of the consideration exchanged by the parties in respect of the Agreement. Notwithstanding anything to the contrary in the Agreement, any notices required or permitted to be given by ColdQuanta to Customer under this DPA may be given (a) in accordance with any notice clause of the Agreement; (b) to ColdQuanta's primary points of contact with Customer; or (c) to any email provided by Customer for the purpose of providing it with Service-related communications or alerts. Customer is solely responsible for ensuring that such email addresses are valid.

ANNEX 1 TO DPA

EU ANNEX

1. Processing of Data

(a) Subject Matter and Details of Processing. The parties acknowledge and agree that (i) the subject matter of the Processing under the Agreement is ColdQuanta's provision of the Service; (ii) the duration of the Processing is from ColdQuanta's receipt of Personal Data until deletion of all Personal Data by ColdQuanta in accordance with the Agreement; (iii) the nature and purpose of the Processing is to provide the Service; (iv) the data subjects to whom the Personal Data pertains are individuals about whom ColdQuanta Processes in connection with the Services; and (v) the categories of personal data are provided by Customer or its users in connection with the Services.

(b) Roles and Regulatory Compliance; Authorization. The parties acknowledge and agree that (a) ColdQuanta is a Processor of that Personal Data under European Data Protection Laws; (b) Customer is a controller (or a processor acting on the instructions of a controller) of that Personal Data under European Data Protection Laws; and (c) each party will comply with the obligations applicable to it in such role under the European Data Protection Laws with respect to the Processing of that Personal Data. If Customer is a processor, Customer represents and warrants to ColdQuanta that Customer's instructions and actions with respect to Personal Data, including its appointment of ColdQuanta as another processor, have been authorized by the relevant controller.

(c) ColdQuanta's Compliance with Instructions. ColdQuanta will only Process Personal Data in accordance with Customer's instructions stated in this DPA unless European Data Protection Laws require otherwise, in which case ColdQuanta will notify Customer (unless that law prohibits ColdQuanta from doing so on important grounds of public interest).

(d) Data Deletion. Customer instructs ColdQuanta to delete all Personal Data from ColdQuanta's systems upon termination of Customer's access to the Service, unless European Data Protection Laws requires otherwise.

2. Data Security

(a) ColdQuanta Security Measures, Controls and Assistance

(i) ColdQuanta Security Assistance. ColdQuanta will (taking into account the nature of the Processing of Personal Data and the information available to ColdQuanta) provide Customer with reasonable assistance necessary for Customer to comply with its obligations in respect of Personal Data under European Data Protection Laws, including Articles 32 to 34 (inclusive) of the GDPR, by (a) implementing and maintaining the Security Measures; (b) complying with the terms of Section 4(b) (Information Security Incidents) of the DPA; and (c) complying with this Annex 1.

(ii) Security Compliance by ColdQuanta Staff. ColdQuanta will grant access to Personal Data only to personnel who need such access for the scope of their job duties, and are subject to appropriate confidentiality arrangements.

(b) Reviews and Audits of Compliance

(i) Customer may audit ColdQuanta's compliance with its obligations under this DPA up to once per year and on such other occasions as may be required by European Data Protection Laws, including where mandated by Customer's supervisory authority. ColdQuanta will contribute to such audits by providing Customer or Customer's supervisory authority with the information and assistance reasonably necessary to conduct the audit.

(ii) If a third party is to conduct the audit, ColdQuanta may object to the auditor if the auditor is, in ColdQuanta's reasonable opinion, not independent, a competitor of ColdQuanta, or otherwise manifestly unsuitable. Such objection by ColdQuanta will require Customer to appoint another auditor or conduct the audit itself.

(iii) To request an audit, Customer must submit a detailed proposed audit plan to ColdQuanta at least two weeks in advance of the proposed audit date and any third party auditor must sign a customary non-disclosure agreement mutually acceptable to the parties (such acceptance not to be unreasonably withheld) providing for the confidential treatment of all information exchanged in connection with the audit and any reports regarding the results or findings thereof. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. ColdQuanta will review the proposed audit plan and provide Customer with any concerns or questions (for example, any request for information that could compromise ColdQuanta security, privacy, employment or other relevant policies). ColdQuanta will work cooperatively with Customer to agree on a final audit plan. Nothing in this Section 2(b) shall require ColdQuanta to breach any duties of confidentiality.

(iv) 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 ColdQuanta has confirmed there are no known material changes in the controls audited, Customer agrees to accept such report in lieu of requesting an audit of such controls or measures.

(v) The audit must be conducted during regular business hours, subject to the agreed final audit plan and ColdQuanta's safety, security or other relevant policies, and may not unreasonably interfere with ColdQuanta business activities.

(vi) Customer will promptly notify ColdQuanta of any non-compliance discovered during the course of an audit and provide ColdQuanta any audit reports generated in connection with any audit under this Section 2(b), unless prohibited by European Data Protection Laws or otherwise instructed by a supervisory authority. Customer may use the audit reports only for the purposes of meeting Customer's regulatory audit requirements and/or confirming compliance with the requirements of this DPA.

(vii) Any audits are at Customer's sole expense. Customer shall reimburse ColdQuanta for any time expended by ColdQuanta or its Third Party Subprocessors in connection with any audits or inspections under this Section 2(b) at ColdQuanta's then-current professional services rates, which shall be made available to Customer upon request. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit. Nothing in this DPA shall be construed to require ColdQuanta to furnish more information about its Third Party Subprocessors in connection with such audits than such Third Party Subprocessors make generally available to their customers.

3. Impact Assessments and Consultations

ColdQuanta will (taking into account the nature of the Processing and the information available to ColdQuanta) reasonably assist Customer in complying with its obligations under Articles 35 and 36 of the GDPR, by (a) making available documentation describing relevant aspects of ColdQuanta's information security program and the security measures applied in connection therewith; and (b) providing the other information contained in the Agreement, including this DPA.

4. Data Transfers

(a) Data Processing Facilities. ColdQuanta may, subject to Section 4(b) (Transfers out of the EEA), store and Process Personal Data in the United States or anywhere ColdQuanta or its Subprocessors maintains facilities.

(b) Transfers out of the EEA. If Customer transfers Personal Data out of the EEA to ColdQuanta in a country not deemed by the European Commission to have adequate data protection, such transfer will be governed by the Standard Contractual Clauses, the terms of which are hereby incorporated into this DPA. In furtherance of the foregoing, the parties agree that:

(i) for purposes of the Standard Contractual Clauses, (a) Customer will act as the data exporter and (b) ColdQuanta will act as the data importer;

(ii) for purposes of Appendix 1 to the Standard Contractual Clauses, the categories of data subjects, data, special categories of data (if appropriate), and the Processing operations shall be as set out in Section 1(a) to this Annex 1 (Subject Matter and Details of Processing);

(iii) for purposes of Appendix 2 to the Standard Contractual Clauses, the technical and organizational measures shall be the Security Measures;

(iv) upon data exporter's request under the Standard Contractual Clauses, data importer will provide the copies of the subprocessor agreements that must be sent by the data importer to the data exporter pursuant to Clause 5(j) of the Standard Contractual Clauses, and that data importer may remove or redact all commercial information or clauses unrelated the Standard Contractual Clauses or their equivalent beforehand;

(v) the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be performed in accordance with Section 2(b) of this Annex 1 (Reviews and Audits of Compliance) and satisfy the Parties' rights and obligations under the Standard Contractual Clauses;

(vi) Customer agrees that the provisions of Section 4(b) (Information Security Incidents) satisfy the requirements of the Standard Contractual Clauses between Customer and ColdQuanta under Clause 5(d)(ii).

(vii) Customer's authorizations in Section 5 of this Annex 1 (Subprocessors) will constitute Customer's prior written consent to the subcontracting by ColdQuanta of the Processing of Personal Data if such consent is required under Clauses 5(h) and 11(1) of the Standard Contractual Clauses; and

(viii) certification of deletion of Personal Data as described in Clause 12(1) of the Standard Contractual Clauses shall be provided upon Customer's request;

(c) Notwithstanding the foregoing, the Standard Contractual Clauses (or obligations the same as those under the Standard Contractual Clauses) will not apply to the extent an alternative recognized compliance standard for the lawful transfer of Personal Data outside the EEA (e.g., binding corporate rules) applies to the transfer.

5. Subprocessors

(a) Consent to Subprocessor Engagement. Customer specifically authorizes the engagement of ColdQuanta's Affiliates as Subprocessors and generally authorizes the engagement of any other third parties as Subprocessors ("Third Party Subprocessors").

(b) Information about Subprocessors. Information about Subprocessors, including their functions and locations, is available at: [URL] (as may be updated by ColdQuanta from time to time) or such other website address as ColdQuanta may provide to customer from time to time (the "Subprocessor Site").

(c) Requirements for Subprocessor Engagement. When engaging any Subprocessor, ColdQuanta will enter into a written contract with such Subprocessor containing data protection obligations not less protective than those in this DPA with respect to Personal Data to the extent applicable to the nature of the services provided by such Subprocessor. ColdQuanta shall be liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

(d) Opportunity to Object to Subprocessor Changes. When ColdQuanta engages any new Third Party after the effective date of the Agreement, ColdQuanta will notify Customer of the engagement (including the name and location of the relevant Subprocessor and the activities it will perform) by updating Subprocessor Site or by other written means. If Customer objects to such engagement in a written notice to ColdQuanta within 15 days after being informed of the engagement on reasonable grounds relating to the protection of Personal Data, Customer and ColdQuanta will work together in good faith to find a mutually acceptable resolution to address such objection. If the parties are unable to reach a mutually acceptable resolution within a reasonable timeframe, Customer may, as its sole and exclusive remedy, terminate the Agreement and cancel the Service by providing written notice to ColdQuanta.

ANNEX 2 TO DPA

CALIFORNIA ANNEX

1. For purposes of this Annex 2, the terms "business," "commercial purpose," "sell" and "service provider" shall have the respective meanings given thereto in the CCPA, and "personal information" shall mean Personal Data that constitutes personal information governed by the CCPA.

2. It is the parties' intent that with respect to any personal information, ColdQuanta is a service provider. ColdQuanta shall not (a) sell any personal information; (b) retain, use or disclose any personal information for any purpose other than for the specific purpose of providing the Service, including retaining, using, or disclosing the personal information for a commercial purpose other than the provision of the Service; or (c) retain, use or disclose the personal information outside of the direct business relationship between ColdQuanta and Customer. ColdQuanta hereby certifies that it understands its obligations under this Section 2 and will comply with them.

3. The parties acknowledge that ColdQuanta's retention, use and disclosure of personal information authorized by Customer's instructions stated in the DPA are integral to ColdQuanta's provision of the Services and the business relationship between the parties.

ANNEX 3 TO DPA

SECURITY MEASURES

1. Organizational management and dedicated staff responsible for the development, implementation and maintenance of the ColdQuanta's information security program.

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

3. Data security controls which include, at a minimum, logical segregation of data, restricted (e.g. role-based) access and monitoring, and utilization of commercially available industry standard encryption technologies for Personal Data that is transmitted over public networks (i.e. the Internet) or when transmitted wirelessly or at rest or stored on portable or removable media (i.e. laptop computers, CD/DVD, USB drives, back-up tapes).

4. Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g. granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review and revoking/changing access promptly when employment terminates or changes in job functions occur).

5. Password controls designed to manage and control password strength, expiration and usage including prohibiting users from sharing passwords and requiring that the ColdQuanta's passwords that are assigned to its employees: (i) be at least eight (8) characters in length, (ii) not be stored in readable format on the ColdQuanta's computer systems; (iii) must have defined complexity; (iv) must have a history threshold to prevent reuse of recent passwords; and (v) newly issued passwords must be changed after first use.

6. System audit or event logging and related monitoring procedures to proactively record user access and system activity.

7. Physical and environmental security of data centers, server room facilities and other areas containing Personal Data designed to: (i) protect information assets from unauthorized physical access, (ii) manage, monitor and log movement of persons into and out of the ColdQuanta's facilities, and (iii) guard against environmental hazards such as heat, fire and water damage.

8. Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from the ColdQuanta's possession.

9. Change management procedures and tracking mechanisms designed to test, approve and monitor all material changes to the ColdQuanta's technology and information assets.

10. Incident management procedures design to allow ColdQuanta to investigate, respond to, mitigate and notify of events related to the ColdQuanta's technology and information assets.

11. Network security controls that provide for the use of enterprise firewalls and layered DMZ architectures, and intrusion detection systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.

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

13. Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergencies or disasters.