Quant Inc.
DPA Setup Page

The Data Processing Agreement (DPA) includes the contents of this DPA Setup Page, including the Key Terms, Schedules and any Additional Terms set forth below. Capitalized terms not defined in this DPA Setup Page have the meanings given in the Data Protection Addendum.

Key Terms

Agreement	This DPA is an Attachment to the Order Form and Agreement between [CUSTOMER NAME] ("Customer") and Quant Inc. ("Provider"), dated [DATE].
DPA Effective Date	Effective the date of the referenced Order Form and Agreement between Customer and Provider.
Subprocesor List[1]	

Sub-Processor	Purpose	Processing Location
Amazon Web Services, Inc.	Cloud Service Provider	U.S.A. and Germany (CS only)
Amazon Web Services EMEA SARL	Cloud Service Provider	Ireland
Okta, Inc.	Authentication Platform	U.S.A. and EU
Clickhouse, Inc.	Data Warehousing	U.S.A. and EU
Google, LLC	Cloud Computing; Back-up Cloud Service Provider; Web service	U.S.A. and Germany
Google, LLC	Cloud Computing; Back-up Cloud Service Provider; Data Analytics Provider; Web service	U.S.A.
Google Cloud EMEA Limited	Back-up Cloud Service Provider	Netherlands
Microsoft, Inc.	Cloud Service Provider for Certain Generative Artificial Intelligence features	U.S.A. and multiple EU locations
OpenAI, L.L.C.	Cloud Service Provider for Certain Generative Artificial Intelligence features	U.S.A, Canada, UK, multiple EU locations, Switzerland, UAE, South Africa and Australia
Twilio, Inc.	Voice and Messaging Services	Based on the location of service provision

Schedules *(attach)*

The following Schedules are incorporated into this DPA:

Schedule 1: Subject Matter and Details of Processing	
Schedule 2: Technical and Organizational Measures	
Schedule 3: Cross-Border Transfer Mechanisms	
Schedule 4: Region-Specific Terms	

Additional Terms

The following additions to or modifications of the Bonterms Data Protection Addendum are agreed by the parties and control in the event of any conflicts:

Specified Notice Period	***Replace*** the definition of "Specified Notice Period" in Section 1.19 with the following: *"Specified Notice Period" is the later of 2 business days or 72 hours.*
Notice of New Subprocessors	***Add*** the following to the end of Section 4.3 (Notice of New Subprocessors): *In addition to email, Provider may notify Customer of changes to the Subprocessor List through the Cloud Service.*

[1] Not all subprocessors will be applicable to all Quant customers and where possible, we restrict data to being processed and stored within an applicable geography.

Bonterms Data Protection Addendum (DPA) (Version 1.0)

This Data Protection Addendum ("**DPA**") is an Attachment to the **Agreement**. Customer and Provider enter into this DPA by executing a DPA Setup Page. Capitalized terms not defined in this DPA are defined in the Agreement or DPA Setup Page.

1. Definitions.

1.1. "**Agreement**" means the Agreement between Customer and Provider incorporating the Bonterms Cloud Terms which is specified on the DPA Setup Page.

1.2. "**Audit**" and "**Audit Parameters**" are defined in Section 9.3 below.

1.3. "**Audit Report**" is defined in Section 9.2 below.

1.4. "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of Processing of Personal Data.

1.5. "**Customer Instructions**" is defined in Section 3.1 below.

1.6. "**Customer Personal Data**" means Personal Data in Customer Data (as defined in the Agreement).

1.7. "**Data Protection Laws**" means all laws and regulations applicable to the Processing of Customer Personal Data under the Agreement, including, as applicable: (i) the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and any binding regulations promulgated thereunder ("**CCPA**"), (ii) the General Data Protection Regulation (Regulation (EU) 2016/679) ("**EU GDPR**" or "**GDPR**"), (iii) the Swiss Federal Act on Data Protection ("**FADP**"), (iv) the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "**UK GDPR**") and (v) the UK Data Protection Act 2018; in each case, as updated, amended or replaced from time to time.

1.8. "**Data Subject**" means the identified or identifiable natural person to whom Customer Personal Data relates.

1.9. "**DPA Effective Date**" is specified on the DPA Setup Page.

1.10. "**DPA Setup Page**" means a separate document executed by Customer and Provider which causes this DPA to become an Attachment to their Agreement.

1.11. "**EEA**" means European Economic Area.

1.12. "**Key Terms**" means Agreement, DPA Effective Date and Subprocessor List as specified by the parties on the DPA Setup Page.

1.13. "**Personal Data**" means information about an identified or identifiable natural person or which otherwise constitutes "personal data", "personal information", "personally identifiable information" or similar terms as defined in Data Protection Laws.

1.14. "**Processing**" and inflections thereof refer to any operation or set of operations that 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.

1.15. "**Processor**" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

1.16. "**Restricted Transfer**" means: (i) where EU GDPR applies, a transfer of Customer Personal Data from the EEA to a country outside the EEA that is not subject to an adequacy determination, (ii) where UK GDPR applies, a transfer of Customer Personal Data from the United Kingdom to any other country that is not subject to an adequacy determination or (iii) where FADP applies, a transfer of Customer Personal Data from Switzerland to any other country that is not subject to an adequacy determination.

1.17. "**Schedules**" means one or more schedules incorporated by the parties in their DPA Setup Page. The default Schedules for this DPA are:

Schedule 1	Subject Matter and Details of Processing
Schedule 2	Technical and Organizational Measures

Schedule 3	Cross-Border Transfer Mechanisms
Schedule 4	Region-Specific Terms

1.18. "**Security Incident**" means any breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data being Processed by Provider.

1.19. "**Specified Notice Period**" is 48 hours.

1.20. "**Subprocessor**" means any third party authorized by Provider to Process any Customer Personal Data.

1.21. "**Subprocessor List**" means the list of Provider's Subprocessors as identified or linked to on the DPA Setup Page.

2. Scope and Duration.

2.1. Roles of the Parties. This DPA applies to Provider as a Processor of Customer Personal Data and to Customer as a Controller or Processor of Customer Personal Data.

2.2. Scope of DPA. This DPA applies to Provider's Processing of Customer Personal Data under the Agreement to the extent such Processing is subject to Data Protection Laws. This DPA is governed by the governing law of the Agreement unless otherwise required by Data Protection Laws.

2.3. Duration of DPA. This DPA commences on the **DPA Effective Date** and terminates upon expiration or termination of the Agreement (or, if later, the date on which Provider has ceased all Processing of Customer Personal Data).

2.4. Order of Precedence. In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) any Standard Contractual Clauses or other measures to which the parties have agreed in Schedule 3 (Cross-Border Transfer Mechanisms) or Schedule 4 (Region-Specific Terms), (2) this DPA and (3) the Agreement. To the fullest extent permitted by Data Protection Laws, any claims brought in connection with this DPA (including its Schedules) will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations, set forth in the Agreement.

3. Processing of Personal Data.

3.1. Customer Instructions.

(a) Provider will Process Customer Personal Data as a Processor only: (i) in accordance with Customer Instructions or (ii) to comply with Provider's obligations under applicable laws, subject to any notice requirements under Data Protection Laws.

(b) "**Customer Instructions**" means: (i) Processing to provide the Cloud Service and perform Provider's obligations in the Agreement (including this DPA) and (ii) other reasonable documented instructions of Customer consistent with the terms of the Agreement.

(c) Details regarding the Processing of Customer Personal Data by Provider are set forth in Schedule 1 (Subject Matter and Details of Processing).

(d) Provider will notify Customer if it receives an instruction that Provider reasonably determines infringes Data Protection Laws (but Provider has no obligation to actively monitor Customer's compliance with Data Protection Laws).

3.2. Confidentiality.

(a) Provider will protect Customer Personal Data in accordance with its confidentiality obligations as set forth in the Agreement.

(b) Provider will ensure personnel who Process Customer Personal Data either enter into written confidentiality agreements or are subject to statutory obligations of confidentiality.

3.3. Compliance with Laws.

(a) Provider and Customer will each comply with Data Protection Laws in their respective Processing of Customer Personal Data.

(b) Customer will comply with Data Protection Laws in its issuing of Customer Instructions to Provider. Customer will

ensure that it has established all necessary lawful bases under Data Protection Laws to enable Provider to lawfully Process Customer Personal Data for the purposes contemplated by the Agreement (including this DPA), including, as applicable, by obtaining all necessary consents from, and giving all necessary notices to, Data Subjects.

3.4. Changes to Laws. The parties will work together in good faith to negotiate an amendment to this DPA as either party reasonably considers necessary to address the requirements of Data Protection Laws from time to time.

4. Subprocessors.

4.1. Use of Subprocessors.

(a) Customer generally authorizes Provider to engage Subprocessors to Process Customer Personal Data. Customer further agrees that Provider may engage its Affiliates as Subprocessors.

(b) Provider will: (i) enter into a written agreement with each Subprocessor imposing data Processing and protection obligations substantially the same as those set out in this DPA and (ii) remain liable for compliance with the obligations of this DPA and for any acts or omissions of a Subprocessor that cause Provider to breach any of its obligations under this DPA.

4.2. Subprocessor List. Provider will maintain an up-to-date list of its Subprocessors, including their functions and locations, as specified in the **Subprocessor List**.

4.3. Notice of New Subprocessors. Provider may update the **Subprocessor List** from time to time. At least 30 days before any new Subprocessor Processes any Customer Personal Data, Provider will add such Subprocessor to the **Subprocessor List** and notify Customer through email or other means specified on the DPA Setup Page.

4.4. Objection to New Subprocessors.

(a) If, within 30 days after notice of a new Subprocessor, Customer notifies Provider in writing that Customer objects to Provider's appointment of such new Subprocessor based on reasonable data protection concerns, the parties will discuss such concerns in good faith.

(b) If the parties are unable to reach a mutually agreeable resolution to Customer's objection to a new Subprocessor, Customer, as its sole and exclusive remedy, may terminate the Order for the affected Cloud Service for convenience and Provider will refund any prepaid, unused fees for the terminated portion of the Subscription Term.

5. Security.

5.1. Security Measures. Provider will implement and maintain reasonable and appropriate technical and organizational measures, procedures and practices, as appropriate to the nature of the Customer Personal Data, that are designed to protect the security, confidentiality, integrity and availability of Customer Personal Data and protect against Security Incidents, in accordance with Provider's Security Measures referenced in the Agreement and as further described in Schedule 2 (Technical and Organizational Measures). Provider will regularly monitor its compliance with its Security Measures and Schedule 2 (Technical and Organizational Measures).

5.2. Incident Notice and Response.

(a) Provider will implement and follow procedures to detect and respond to Security Incidents.

(b) Provider will: (i) notify Customer without undue delay and, in any event, not later than the Specified Notice Period, after becoming aware of a Security Incident affecting Customer and (ii) make reasonable efforts to identify the cause of the Security Incident, mitigate the effects and remediate the cause to the extent within Provider's reasonable control.

(c) Upon Customer's request and taking into account the nature of the applicable Processing, Provider will assist Customer by providing, when available, information reasonably necessary for Customer to meet its Security Incident notification obligations under Data Protection Laws.

(d) Customer acknowledges that Provider's notification of a Security Incident is not an acknowledgement by Provider of its fault or liability.

(e) Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful login attempts, pings, port scans, denial of service attacks or other network attacks on firewalls or networked systems.

5.3. Customer Responsibilities.

(a) Customer is responsible for reviewing the information made available by Provider relating to data security and

making an independent determination as to whether the Cloud Service meets Customer's requirements and legal obligations under Data Protection Laws.

(b) Customer is solely responsible for complying with Security Incident notification laws applicable to Customer and fulfilling any obligations to give notices to government authorities, affected individuals or others relating to any Security Incidents.

6. **Data Protection Impact Assessment**. Upon Customer's request and taking into account the nature of the applicable Processing, to the extent such information is available to Provider, Provider will assist Customer in fulfilling Customer's obligations under Data Protection Laws to carry out a data protection impact or similar risk assessment related to Customer's use of the Cloud Service, including, if required by Data Protection Laws, by assisting Customer in consultations with relevant government authorities.

7. **Data Subject Requests**.

7.1. Assisting Customer. Upon Customer's request and taking into account the nature of the applicable Processing, Provider will assist Customer by appropriate technical and organizational measures, insofar as possible, in complying with Customer's obligations under Data Protection Laws to respond to requests from individuals to exercise their rights under Data Protection Laws, provided that Customer cannot reasonably fulfill such requests independently (including through use of the Cloud Service).

7.2. Data Subject Requests. If Provider receives a request from a Data Subject in relation to the Data Subject's Customer Personal Data, Provider will notify Customer and advise the Data Subject to submit the request to Customer (but not otherwise communicate with the Data Subject regarding the request except as may be required by Data Protection Laws), and Customer will be responsible for responding to any such request.

8. **Data Return or Deletion**.

8.1. During Subscription Term. During the Subscription Term, Customer may, through the features of the Cloud Service or such other means specified on the DPA Setup Page, access, return to itself or delete Customer Personal Data.

8.2. Post Termination.

(a) Following termination or expiration of the Agreement, Provider will, in accordance with its obligations under the Agreement, delete all Customer Personal Data from Provider's systems.

(b) Deletion will be in accordance with industry-standard secure deletion practices. Provider will issue a certificate of deletion upon Customer's request.

(c) Notwithstanding the foregoing, Provider may retain Customer Personal Data: (i) as required by Data Protection Laws or (ii) in accordance with its standard backup or record retention policies, provided that, in either case, Provider will (x) maintain the confidentiality of, and otherwise comply with the applicable provisions of this DPA with respect to, retained Customer Personal Data and (y) not further Process retained Customer Personal Data except for such purpose(s) and duration specified in such applicable Data Protection Laws.

9. **Audits**.

9.1. Provider Records Generally. Provider will keep records of its Processing in compliance with Data Protection Laws and, upon Customer's request, make available to Customer any records reasonably necessary to demonstrate compliance with Provider's obligations under this DPA and Data Protection Laws.

9.2. Third-Party Compliance Program.

(a) Provider will describe its third-party audit and certification programs (if any) and make summary copies of its audit reports (each, an "**Audit Report**") available to Customer upon Customer's written request at reasonable intervals (subject to confidentiality obligations).

(b) Customer may share a copy of Audit Reports with relevant government authorities as required upon their request.

(c) Customer agrees that any audit rights granted by Data Protection Laws will be satisfied by Audit Reports and the procedures of Section 9.3 (Customer Audit) below.

9.3. Customer Audit.

(a) Subject to the terms of this Section 9.3, Customer has the right, at Customer's expense, to conduct an audit of reasonable scope and duration pursuant to a mutually agreed-upon audit plan with Provider that is consistent with the Audit Parameters (an "**Audit**").

(b) Customer may exercise its Audit right: (i) to the extent Provider's provision of an Audit Report does not provide sufficient information for Customer to verify Provider's compliance with this DPA or the parties' compliance with Data Protection Laws, (ii) as necessary for Customer to respond to a government authority audit or (iii) in connection with a Security Incident.

(c) Each Audit must conform to the following parameters ("**Audit Parameters**"): (i) be conducted by an independent third party that will enter into a confidentiality agreement with Provider, (ii) be limited in scope to matters reasonably required for Customer to assess Provider's compliance with this DPA and the parties' compliance with Data Protection Laws, (iii) occur at a mutually agreed date and time and only during Provider's regular business hours, (iv) occur no more than once annually (unless required under Data Protection Laws or in connection with a Security Incident), (v) cover only facilities controlled by Provider, (vi) restrict findings to Customer Personal Data only and (vii) treat any results as confidential information to the fullest extent permitted by Data Protection Laws.

10. Cross-Border Transfers/Region-Specific Terms.

10.1. Cross-Border Data Transfers.

- Provider (and its Affiliates) may Process and transfer Customer Personal Data globally as necessary to provide the Cloud Service.
- If Provider engages in a Restricted Transfer, it will comply with Schedule 3 (Cross-Border Transfer Mechanisms).

10.2. Region-Specific Terms. To the extent that Provider Processes Customer Personal Data protected by Data Protection Laws in one of the regions listed in Schedule 4 (Region-Specific Terms), then the terms specified therein with respect to the applicable jurisdiction(s) will apply in addition to the terms of this DPA.

Schedule 1: Subject Matter and Details of Processing

Customer / 'Data Exporter' Details

Name:	**Customer, as specified in the Order Form.**
Contact details for data protection:	The individual and/or email specified in the Cover Page or the Order Form, as applicable.
Main address:	The Customer's address specified in the Cover Page or the Order Form, as applicable.
Role:	Controller

Provider / 'Data Importer' Details

Name:	**Provider, as specified in the Order Form.**
Contact details for data protection:	Name: Quant Inc. Privacy and Security Team Email: privacy@quant.ai
Main address:	The Provider's address, as specified in the Cover Page or the Order Form, as applicable.
Provider activities:	Quant will Process Personal Data as necessary to provide the Services pursuant to the Agreement, as further specified in the applicable Order Form, and as further instructed by customer in customer's use of the Services.
Role:	Processor

Details of Processing

Categories of Data Subjects:	You may submit Personal Data in the course of using the Services, the extent of which is determined and controlled by you in your sole discretion, and which may include, but is not

	limited to Personal Data relating to the following categories of Data Subjects: • Your users and other end users including your employees, contractors, collaborators, customers, prospects, suppliers, and subcontractors. • Data Subjects may also include individuals attempting to communicate with or transfer Personal Data to your end users. • Your users who are authorized by you to use the Services.
Categories of Customer Personal Data:	The types of personal data processed — the extent of which is determined and controlled by Controller in its sole discretion — may include: • First and last name • Title • Position • Employer • Contact information (company, email, phone, physical business address) • Identification Data (notably email addresses and phone numbers) • Electronic identification data (notably IP addresses and mobile device IDs)
Sensitive Categories of Data and additional associated restrictions/safeguards:	NONE.
Frequency of transfer:	The Processing will continue until the expiration or termination of the Main Agreement.
Nature of the Processing:	Processor will process personal data as necessary to perform the Cloud Service pursuant to the Order Form, the Agreement, and as further instructed by the Controller in its use of the Cloud Service.
Purpose of the Processing:	Performance of the Cloud Services pursuant to the applicable Order Form and the Main Agreement.
Duration of Processing / retention period:	Processing will continue until the expiration or termination of the Agreement. In accordance with the timeframes specified in the Agreement, Processor will securely destroy (in accordance with standard industry practices for deletion of personal data) all copies of Controller's personal data. Upon Controller's request, Processor will promptly deliver to Controller an export of Controller's personal data (in CSV or similar format) within thirty (30) calendar days and, if Customer also requests deletion of Controller's personal data, will carry that out as set forth above. Tapes, printed output, optical disks, and other physical media will be physically destroyed by a secure method and by a recognized provider.
Transfers to Subprocessors:	Standard Contractual Clauses approved by the European Commission Decision of 4 June 2021 (as amended from time to time), for the transfer of personal data from the EEA or adequate country to a third country. International Data Transfer Addendum issued by the United Kingdom's Information Commissioner's Office under Section 119A of the Data Protection Act 2018, effective from 21 March 2022.

Schedule 2: Technical and Organizational Measures

Please visit https://quant.ai/security for the latest Provider security information datasheet, in addition to the measures listed below. Provider may modify the Security Information Datasheet or Provider's information security and privacy measures to reflect new technical and organizational measures or changing practices, but the modifications may not be retroactive or materially decrease Provider's overall obligations during a Subscription Term.

1. Measures of pseudonymization and encryption of personal data.
   - Quant requires full-disk hard drive encryption using AES-256 for all employee computers, and uses role-based access control, multi-factor authentication, and account management procedures to control access to Customer Data.
   - Quant encrypts data in transit and at rest using hybrid encryption techniques that align with NIST Special Publication 800-53.
   - Customer Data at rest is encrypted using the AES-256 algorithm
   - Quant uses TLS version 1.2 or higher to protect all data in transit.
   - For email security, Quant uses opportunistic TLS encryption.
   - Customer Data that is hosted with AWS is encrypted at rest as described in AWS's documentation available at https://aws.amazon.com/compliance/data-center/controls/
   - AWS log-in credentials and private keys generated by the Service are for Quant's internal use only and stored in a secret vault.
   - Encryption keys are rotated annually at a minimum, performed by AWS Key Management Service
2. Measures for ensuring ongoing confidentiality, integrity, availability, and resilience of processing systems and services.
   - Quant maintains a record of personnel authorized to access systems that contain Customer Data.
   - Privileged access requires a formal account management and access control procedure that requires review and approval from a manager or designated executives.
   - Quant deactivates authentication credentials of individuals promptly following the termination of their employment or services termination or a role transfer that no longer requires access to Customer Data.
   - Quant's personnel are contractually and legally obligated to maintain the confidentiality of Customer Data and this obligation continues after their employment or service ends.
   - Employees complete mandatory annual security training, which covers data privacy and governance, data protection, confidentiality, social engineering, password policies, and information security.
   - Quant requires all employees follow documented password polies for all employees and follows NIST best practices.
   - Quant web application account passwords are hashed when stored.
   - Quant web application sessions expire after a customer configurable inactivity timer which default to 30 minutes.
3. Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
   - Quant maintains geographically distributed data centers using AWS cloud hosting infrastructure.
   - Quant's information systems use security logs and alerting.
   - Quant's incident reporting and response procedure aligns with NIST SP 800-61 guidance on handling incidents, including steps for breach notification.
   - All incidents are logged in an incident tracking system that is subject to annual audit.
   - Quant has a business continuity and disaster recovery plan that incorporates input from periodic risk assessments, vulnerability scanning, and threat analysis.
   - Quant conducts an incident response and business continuity and disaster recovery test annually that is used to inform the ongoing risk assessment and management process.

4. Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing.
   - Quant conducts regular risk assessments and monitors the effectiveness of its safeguards, controls, and systems, through regular vulnerability scans, penetration testing, and intrusion detection.
   - Quant's vulnerability management program includes an independent testing team to perform vulnerability scanning to assess its internal and external network environments against emerging security threats.
   - Quant implements server protection on the production environment and endpoint protection on laptop/desktop endpoints, including continuously updated antivirus software.
   - The servers that host the Quant Service are scanned for viruses and malware on a weekly basis.
   - The Quant web application, network segmentation, and interconnections are protected by firewalls.

- Quant services operate in separate, virtual networks that are isolated from other external traffic.
- Quant's corporate equipment is protected to reduce the risks from environmental threats, hazards, and opportunities for unauthorized access.
- Sub-processors undergo onboarding due diligence to ensure compliance with security and privacy requirements, laws, and regulations. To the extent applicable, sub-processors are required to sign a Data Processing Addendum that includes compliance with data protection laws and our customer agreements.

5. Measures for user identification and authorization.
   - Quant uses commercially reasonable practices to identify and authenticate users accessing its information systems. These processes are designed to maintain the confidentiality and integrity of account credentials when they are assigned and distributed and during storage.
   - Quant requires the use of MFA for all remote connections
   - Customers manage their own password complexity, MFA and SSO/SAML 2.0 requirements.

6. Measures for the protection of Customer Data during transmission.
   - Customer Data is encrypted in transit.
   - All communications between the Customer and Quant, as well as all third-party applications, take place over a secure HTTPS connection using TLS 1.2 or higher protocol.
   - The Quant production environments include logical and physical separation of components using network segmentation, software defined networking technologies (where appropriate) and firewalls.
   - Customer Production, dev, testing, and staging environments are logically separated from each other and from internal Quant networks.
   - All connections between Quant internal networks and the Internet or any other publicly accessible network include an approved firewall or related access control system.

7. Measures for the protection of Customer Data during storage.
   - Customer Data is hosted by AWS. Quant maintains complete administrative control over its virtual servers.
   - AWS Key Management System is used to encrypt data in our cloud infrastructure using FIPS 140-2 validated hardware security modules to protect keys from unauthorized access.
   - Customer Data within Quant's multi-tenant environments is logically segregated and attempts to access Customer Data outside allowed domain boundaries are prevented and logged.
   - The Quant web application runs antivirus scans regularly to detect malicious files present in the production environment and all personal data access is logged.

8. Measures for ensuring physical security of locations where Customer Data is processed.
   - Physical access to data hosting facilities is documented and managed by AWS.
   - AWS uses commercially reasonable systems and measures to protect against loss of data due to power supply failure and maintains documentation of the same.
   - Quant limits access to its corporate offices to identified authorized individuals who require access for the performance of their job function and authorized, escorted visitors.
   - Quant offices have no direct access to Customer production, development, testing, and staging and operate on a zero trust principle.
   - Customers do not provide any physical media to Quant.
   - Access to customer data via digital media is limited to employees who require access. The IT Team administers employees' access, which must be approved based on job role.
   - Quant uses commercially reasonable processes to securely destroy customer digital media in accordance with the Customer Agreement.
   - Access cards and/or keys are not shared.
   - Access cards and/or keys that are no longer required are returned to the IT Team or disabled.
   - Quant employees are responsible for notifying the IT Team within 24 hours if their access cards and/or keys are lost, stolen, or compromised.
   - Cards and/or keys have no identifying information coded into them.

9. Measures for ensuring events logging.
   - Event and system access logs are monitored and reviewed periodically.
   - User activity metrics and logs, configuration changes, deletions, and updates are written automatically to audit logs in operational systems.
   - User activity metrics are available to customers within the Quant web application.

- Audit logs maintain timestamp, IP address, specific action taken, and certain requested metadata.
- Certain log events on Quant such as timestamps, IPs, login/logouts, and errors are available to authorized employees for security investigations.
- Notifications and alerts are sent based on the rules configured in the monitoring systems to identify anomalies, suspicious network behavior, abnormal activities, and potential threats.
- Quant has a central security information and event management system and other product tools to monitor the security alerts generated by the Quant Service.

10. Measures for ensuring system configuration, including default configuration.
    - Quant has a configuration management policy to securely control assets, configurations, and changes throughout the software development lifecycle.
    - Quant monitors and logs all changes to in-scope systems to ensure that changes follow the process and to mitigate the risk of undetected changes to the production environment.

11. Measures for internal security governance and IT Management.
    - Quant maintains appropriate documentation describing its security measures and relevant procedures and responsibilities of its personnel.
    - Quant has established an Information Security Management System in accordance with ISO 27001:2022.
    - Managing Quant's information security program is the responsibility of the Governance, Risk, and Compliance team who is authorized by senior management to take all reasonable actions necessary to establish, implement, and manage Quant's information security program.

12. Measures for certification/assurance of processes and products.
    - Quant's system of internal control requires annual independent third-party audits to test the operational effectiveness of its program and practices. Annual audits include SOC 2 Type 2 (Security, Privacy, Confidentiality & Availability).
    - Quant uses independent auditors to review its compliance status for HIPAA and GDPR, attesting to our Data Processing Agreement 11 / 12 Confidential and Proprietary commitment to safeguard the confidentiality, integrity, and privacy of information stored and processed in our Service.
    - AWS certifies or attests to: (A) SOC 1, 2, and 3; (B) ISO 27001, 27017, 27018, 27701, and 9001; (C) Cloud Security Alliance Security, Trust, Assurance and Risk Cloud Control Matrix v3.0.1; (D) FedRAMP; and (E) FIPS 140-2. Further information can be found at https://aws.amazon.com/compliance/data-center/controls/.

13. Measures for ensuring data minimization.
    - Quant only collects data that the Customer chooses to provide as part of receiving the Services.
    - Quant returns or destroys Customer Data at the Customer's request in accordance with the Agreement.

14. Measures for ensuring data quality.
    - Quant will assist customers acting on a data subject access request to amend or correct information when required
    - Software releases and updates/patches to Quant production environments are tested for functionality and security, including any significant modifications, major enhancements, and new systems, prior to deployment.

15. Measures for ensuring limited data retention.
    - Customer Data is retained as per the contractual terms agreed with the Customer and as required by applicable privacy law.
    - Customer has the ability to determine the retention times and may configure such retention times in the Quant application
    - After termination of a Subscription, Customer Data is deleted from the production environment within a commercially reasonable timeframe.
16. Measures for ensuring accountability.
    - Events and audit trails related to Quant Service and system access are logged and regularly reviewed.
    - Quant adopts the Three Lines of Defense governance model for its system of internal control for transparent management of compliance obligations and risks.
17. Measures for allowing data portability and ensuring erasure.
    - Customers can export Customer Data at any time to standard machine- readable formats
    - Quant allows individuals to exercise their privacy rights under applicable privacy law.

Schedule 3: Cross-Border Transfer Mechanisms

1. **Definitions**. Capitalized terms not defined in this Schedule are defined in the DPA.

   1.1. "**EU Standard Contractual Clauses**" or "**EU SCCs**" means the Standard Contractual Clauses approved by the European Commission in decision 2021/914.

   1.2. "**UK International Data Transfer Agreement**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force as of March 21, 2022.

   1.3. In addition:

"**Designated EU Governing Law**" means:	Republic of Ireland
"**Designated EU Member State**" means:	Republic of Ireland

2. **EU Transfers**. Where Customer Personal Data is protected by EU GDPR and is subject to a Restricted Transfer, the following applies:

   2.1. The EU SCCs are hereby incorporated by reference as follows:

   (a) Module 2 (Controller to Processor) applies where Customer is a Controller of Customer Personal Data and Provider is a Processor of Customer Personal Data;

   (b) Module 3 (Processor to Processor) applies where Customer is a Processor of Customer Personal Data (on behalf of a third-party Controller) and Provider is a Processor of Customer Personal Data;

   (c) Customer is the "data exporter" and Provider is the "data importer"; and

   (d) by entering into this DPA, each party is deemed to have signed the EU SCCs (including their Annexes) as of the DPA Effective Date.

   2.2. For each Module, where applicable the following applies:

   (a) the optional docking clause in Clause 7 does not apply;

   (b) in Clause 9, Option 2 will apply, the minimum time period for prior notice of Subprocessor changes shall be as set out in Section 4.3 of this DPA, and Provider shall fulfill its notification obligations by notifying Customer of any Subprocessor changes in accordance with Section 4.3 of this DPA;

   (c) in Clause 11, the optional language does not apply;

   (d) in Clause 13, all square brackets are removed with the text remaining;

   (e) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Designated EU Governing Law;

   (f) in Clause 18(b), disputes will be resolved before the courts of the Designated EU Member State;

   (g) Schedule 1 (Subject Matter and Details of Processing) to this DPA contains the information required in Annex 1 of the EU SCCs; and

   (h) Schedule 2 (Technical and Organizational Measures) to this DPA contains the information required in Annex 2 of the EU SCCs.

   2.3. Where context permits and requires, any reference in this DPA to the EU SCCs shall be read as a reference to the EU SCCs as modified in the manner set forth in this Section 2.

3. **Swiss Transfers**. Where Customer Personal Data is protected by the FADP and is subject to a Restricted Transfer, the following applies:

   3.1. The EU SCCs apply as set forth in Section 2 (EU Transfers) of this Schedule 3 with the following modifications:

   (a) in Clause 13, the competent supervisory authority shall be the Swiss Federal Data Protection and Information Commissioner;

   (b) in Clause 17 (Option 1), the EU SCCs will be governed by the laws of Switzerland;

   (c) in Clause 18(b), disputes will be resolved before the courts of Switzerland;

(d) the term Member State must not be interpreted in such a way as to exclude Data Subjects in Switzerland from enforcing their rights in their place of habitual residence in accordance with Clause 18(c); and

(e) all references to the EU GDPR in this DPA are also deemed to refer to the FADP.

4. **UK Transfers**. Where Customer Personal Data is protected by the UK GDPR and is subject to a Restricted Transfer, the following applies:

4.1. The EU SCCs apply as set forth in Section 2 (EU Transfers) of this Schedule 3 with the following modifications:

(a) each party shall be deemed to have signed the "UK Addendum to the EU Standard Contractual Clauses" ("**UK Addendum**") issued by the Information Commissioner's Office under section 119 (A) of the Data Protection Act 2018;

(b) the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of Customer Personal Data;

(c) in Table 1 of the UK Addendum, the parties' key contact information is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA;

(d) in Table 2 of the UK Addendum, information about the version of the EU SCCs, modules and selected clauses which this UK Addendum is appended to are located above in this Schedule 3;

(e) in Table 3 of the UK Addendum:

(i) the list of parties is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA;

(ii) the description of transfer is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA;

(iii) Annex II is located in Schedule 2 (Technical and Organizational Measures) to this DPA; and

(iv) the list of Subprocessors is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA.

(f) in Table 4 of the UK Addendum, both the Importer and the Exporter may end the UK Addendum in accordance with its terms (and the respective box for each is deemed checked); and

(g) in Part 2: 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 section 119 (A) of the Data Protection Act 2018 on 2 February 2022, as it is revised under section 18 of those Mandatory Clauses.

Schedule 4: Region-Specific Terms

California

1. **Definitions**. CCPA and other capitalized terms not defined in this Schedule are defined in the DPA.

1.1. "business purpose", "commercial purpose", "personal information", "sell", "service provider" and "share" have the meanings given in the CCPA.

1.2. The definition of "Data Subject" includes "consumer" as defined under the CCPA.

1.3. The definition of "Controller" includes "business" as defined under the CCPA.

1.4. The definition of "Processor" includes "service provider" as defined under the CCPA.

2. **Obligations**.

2.1. Customer is providing the Customer Personal Data to Provider under the Agreement for the limited and specific business purposes of providing the Cloud Service as described in Schedule 1 (Subject Matter and Details of Processing) to this DPA and otherwise performing under the Agreement.

2.2. Provider will comply with its applicable obligations under the CCPA and provide the same level of privacy protection to Customer Personal Data as is required by the CCPA.

2.3. Provider acknowledges that Customer has the right to: (i) take reasonable and appropriate steps under Section 9 (Audits) of this DPA to help to ensure that Provider's use of Customer Personal Data is consistent with Customer's obligations under the CCPA, (ii) receive from Provider notice and assistance under Section 7 (Data Subject Requests) of this DPA regarding consumers' requests to exercise rights under the CCPA and (iii) upon notice, take reasonable and appropriate

steps to stop and remediate unauthorized use of Customer Personal Data.

2.4. Provider will notify Customer promptly after it makes a determination that it can no longer meet its obligations under the CCPA.

2.5. Provider will not retain, use or disclose Customer Personal Data: (i) for any purpose, including a commercial purpose, other than the business purposes described in Section 2.1 of this Section A (California) of Schedule 4 or (ii) outside of the direct business relationship between Provider with Customer, except, in either case, where and to the extent permitted by the CCPA.

2.6. Provider will not sell or share Customer Personal Data received under the Agreement.

2.7. Provider will not combine Customer Personal Data with other personal information except to the extent a service provider is permitted to do so by the CCPA.

Activity Prior to January 1, 2023. To the extent this Section A (California) of Schedule 4 is in effect prior to January 1, 2023, Provider's obligations hereunder that are required solely by amendments to the CCPA made by the California Privacy Rights Act regarding contractual obligations of service providers shall only apply on and after January 1, 2023.