QUANT

Data Processing Agreement

Last Updated: July 1, 2026

This Data Processing Agreement ("**DPA**") is entered into by and between Quant, Inc., ("**Provider**") and the Customer detailed in the applicable Order Form ("**Customer**") and is effective as of the DPA Effective Date. This DPA is incorporated into and forms part of the Agreement. Capitalized terms used but not defined herein shall have the same meaning ascribed to it in the Agreement.

Key Terms

Key Terms	
Agreement	This DPA is an attachment to the Order Form between Customer and Provider dated [DATE].
DPA Effective Date	Effective as of the date of the referenced Order Form and Agreement between Customer and Provider.
Specified Notice Period	Within 72 hours after becoming aware of a Security Incident affecting Customer.
Privacy Contact	Provider's Privacy & Security Team - privacy@quant.ai

Sub-Processor List

The following sub-processors may process Customer Personal Data in connection with the Services. Processing locations have been verified from each vendor's official sub-processor or privacy disclosure page as of the Last Updated date above. Not all sub-processors will be applicable to all customers. Provider restricts data to applicable geographies where possible.

Official source URLs are listed in the rightmost column. Visit each vendor's page directly for the most current information, as sub-processor lists are updated frequently.

Sub-Processor	Purpose	Processing Location
Amazon Web Services, Inc.	Cloud Computing Data Storage Backup AI/ML Services	Customer's selected AWS Region(s); global regions available in USA, EU, Asia Pacific and more
Google Cloud Platform (Google LLC)	Cloud Computing Data Storage Backup AI/ML Services	Customer's selected GCP region(s); global regions available in USA, EU, Asia Pacific and more
Microsoft Corporation (Azure)	Cloud Computing Data Storage Backup AI/ML Services	Customer's selected Azure region(s); global regions available in USA, EU, Asia Pacific and more
OpenAI, L.L.C.	Generative AI / Large Language Model Services	Worldwide; Customer selected geographies available on a case by case basis
Anthropic, PBC	Generative AI / Large Language Model Services	Worldwide; Customer selected geographies available on a case by case basis
Groq, Inc.	High-Performance AI Inference Services	Worldwide; Customer selected geographies available on a case by case basis
ElevenLabs, Ltd.	AI Voice Synthesis & Text-to-Speech Services	USA (default); EU or India residency available on a case by case basis
Deepgram, Inc.	AI Speech Recognition & Transcription Services	USA (default); EU endpoint available at api.eu.deepgram.com for GDPR-regulated processing

LiveKit, Inc.	Real-Time Audio/Video Communication Infrastructure	Worldwide; Endpoints available in EU, SA, and IN on a case by case basis
MongoDB Inc.	Database as a Service	USA (Default); Customer's selected cloud provider and region on a case by case basis.
Twilio, Inc.	Voice, Messaging & Communications Services	USA (default Region US1); Ireland (EU Region IE1); Australia (AU1); edge locations globally across Americas, Europe, Asia Pacific
Telnyx LLC	Voice, SMS & Communications Platform Services	USA and Worldwide
Okta, Inc.	Identity & Access Management / Authentication	USA (primary); EU on a case by case basis
Atlassian Pty Ltd (Jira & Confluence Cloud)	Project Management & Collaboration Tools	USA
GitHub, Inc. (GitHub Cloud)	Source Code Repository, CI/CD & AI Services	USA

** Provider may update the Sub-Processor List from time to time in accordance with Section 4 of this DPA. Locations shown reflect each vendor's official disclosures and may vary depending on the customer's selected region, service tier, or product features used.*

Schedules Incorporated

Schedule	Title
Schedule 1	Subject Matter and Details of Processing
Schedule 2	Technical and Organizational Measures
Schedule 3	Region-Specific Terms

QUANT

Section 1: Definitions

Capitalized terms used in this DPA have the meanings set forth below. Terms not defined herein have the meanings given in the Agreement.

Defined Terms	
"Agreement"	The master agreement between Customer and Provider incorporating Provider's Cloud Terms as specified in the Order Form.
"Controller"	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.
"Customer Instructions"	Has the meaning given in Section 3.1 of this DPA.
"Customer Personal Data"	Personal Data included in Customer Data as defined in the Agreement.
"Data Protection Laws"	All applicable laws and regulations governing the Processing of Customer Personal Data, including as applicable: (i) CCPA/CPRA; (ii) EU GDPR (Regulation (EU) 2016/679); (iii) Swiss FADP; (iv) UK GDPR; and (v) UK Data Protection Act 2018; in each case as amended from time to time.
"Data Subject"	The identified or identifiable natural person to whom Customer Personal Data relates.
"EEA"	European Economic Area.
"Personal Data"	Any information relating to an identified or identifiable natural person, including "personal data", "personal information", or "personally identifiable information" as defined under applicable Data Protection Laws.
"Processing"	Any operation or set of operations performed on Personal Data, whether by automated means, including collection, recording, storage, adaptation, retrieval, use, disclosure, or erasure.
"Processor"	A natural or legal person, public authority, agency, or other body that Processes Personal Data on behalf of the Controller.
"Restricted Transfer"	A transfer of Customer Personal Data: (i) from the EEA to a non-adequate third country (EU GDPR); (ii) from the UK to a non-adequate country (UK GDPR); or (iii) from Switzerland to a non-adequate country (FADP).
"Security Incident"	Any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data processed by Provider.
"Specified Notice Period"	The later of 2 business days or 72 hours after Provider becomes aware of a Security Incident affecting Customer.
"Sub-processor"	Any third party authorized by Provider to Process Customer Personal Data.
"Sub-processor List"	The list of Provider's Sub-processors set forth in the DPA Setup Page, as updated from time to time.

QUANT

Section 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 either a Controller or Processor of Customer Personal Data, as applicable. Where Customer acts as a Processor on behalf of a third-party Controller, Customer represents that its instructions to Provider are consistent with its obligations to that Controller.

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 applicable Data Protection Laws.

2.3. Duration of DPA

This DPA commences on the DPA Effective Date and continues until the 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, the following order of precedence applies:

- Standard Contractual Clauses or other cross-border transfer mechanisms or Region-Specific Terms (Schedule 4);
- This DPA (including all Schedules);
- The Agreement.

To the fullest extent permitted by Data Protection Laws, claims arising under this DPA are subject to the exclusions and limitations set forth in the Agreement.

Section 3: Processing of Personal Data

3.1. Customer Instructions

Provider will Process Customer Personal Data solely: (a) in accordance with Customer Instructions, or (b) as required to comply with applicable law (subject to any notice requirements under Data Protection Laws).

"Customer Instructions" means: (i) Processing necessary to provide the Cloud Service and perform Provider's obligations under the Agreement; and (ii) other reasonable, documented instructions of Customer consistent with the terms of the Agreement.

Provider will notify Customer promptly if it receives an instruction that Provider reasonably believes infringes Data Protection Laws. Provider has no obligation to actively monitor Customer's compliance with Data Protection Laws.

3.2. Confidentiality

Provider will protect Customer Personal Data in accordance with its confidentiality obligations in the Agreement. Provider will ensure that personnel authorized to Process Customer Personal Data are subject to appropriate confidentiality obligations, whether contractual or statutory.

3.3. Compliance with Laws

Each party will independently comply with Data Protection Laws applicable to its Processing of Customer Personal Data. Customer is responsible for:

- Issuing Customer Instructions that comply with Data Protection Laws;
- Establishing all lawful bases required to enable Provider to Process Customer Personal Data as contemplated by the Agreement;
- Obtaining all necessary consents and providing all required notices to Data Subjects.

3.4. Changes to Laws

The parties will cooperate in good faith to amend this DPA as reasonably necessary to address changes in applicable Data Protection Laws.

QUANT

Section 4: Sub-Processors

4.1. General Authorization

Customer hereby provides general authorization for Provider to engage the Sub-processors listed in the Sub-processor List. Customer further agrees that Provider may engage its Affiliates as Sub-processors. Provider will:

- Enter into a written agreement with each Sub-processor imposing data protection obligations at least as protective as those in this DPA; and
- Remain liable to Customer for the acts and omissions of Sub-processors to the same extent as if Provider performed the Processing directly.

4.2. Sub-processor List Maintenance

Provider will maintain an up-to-date Sub-processor List identifying each Sub-processor, its function, and its processing location. The current list is set forth in the DPA Setup Page of this DPA. Processing locations reflect each vendor's official public disclosures; actual locations may vary based on the customer's selected region or service features.

4.3. Notice of New Sub-Processors

Provider may update the Sub-processor List from time to time. At least 30 days before any new Sub-processor begins Processing Customer Personal Data, Provider will: (a) add the new Sub-processor to the Sub-processor List; and (b) notify Customer via email and/or through the Cloud Service.

4.4. Objection to New Sub-Processors

If Customer has reasonable data protection concerns regarding a new Sub-processor, Customer may object in writing within 30 days of notice. The parties will discuss such concerns in good faith. If no mutually agreeable resolution is reached, Customer's sole and exclusive remedy is to terminate the affected Order for convenience, with a pro-rata refund of prepaid, unused fees.

Section 5: Security

5.1. Security Measures

Provider will implement and maintain appropriate technical and organizational measures designed to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access, as further described in Schedule 2 (Technical and Organizational Measures). Provider will regularly monitor its compliance with these measures.

5.2. Security Incident Response

Provider will implement and maintain procedures to detect and respond to Security Incidents. Upon becoming aware of a Security Incident affecting Customer Personal Data, Provider will:

- Notify Customer without undue delay and, in any event, within the Specified Notice Period;
- Make reasonable efforts to identify the cause, mitigate effects, and remediate the root cause;
- Upon Customer's request, provide information reasonably necessary for Customer to meet its own Security Incident notification obligations.

Provider's notification of a Security Incident does not constitute an admission of fault or liability. Security Incidents exclude unsuccessful attempts that do not compromise Customer Personal Data (e.g., failed logins, port scans, DDoS attacks on firewalls).

5.3. Customer Responsibilities

Customer is responsible for independently evaluating whether the Cloud Service meets its security requirements. Customer is solely responsible for compliance with Security Incident notification obligations applicable to Customer, including notifications to government authorities and affected individuals.

Section 6: Data Subject Rights and Impact Assessments

6.1. Assistance with Data Subject Requests

Upon Customer's request, and taking into account the nature of the Processing, Provider will assist Customer by appropriate technical and organizational measures in responding to Data Subject requests to exercise rights under Data Protection Laws (including rights of access, rectification, erasure, restriction, portability, and objection), to the extent Customer cannot reasonably fulfill such requests independently.

6.2. Handling of Direct Data Subject Requests

If Provider receives a request directly from a Data Subject regarding Customer Personal Data, Provider will:

(a) notify Customer promptly;

(b) advise the Data Subject to submit the request to Customer; and

(c) not otherwise respond to the Data Subject except as required by Data Protection Laws.

6.3. Data Protection Impact Assessments

Upon Customer's request, and to the extent information is available to Provider, Provider will assist Customer in fulfilling its obligations to conduct data protection impact assessments (DPIAs) or similar risk assessments related to Customer's use of the Cloud Service, including assisting with consultations with relevant supervisory authorities where required.

Section 7: Data Return and Deletion

7.1. During Subscription Term

During the Subscription Term, Customer may access, export, or delete Customer Personal Data through the features of the Cloud Service or by such other means as specified in the Order Form.

7.2. Post-Termination

Following expiration or termination of the Agreement, Provider will delete all Customer Personal Data from its systems in accordance with its obligations under the Agreement and using industry-standard secure deletion practices.

Upon Customer's written request, Provider will:

(a) deliver a data export in CSV or similar machine-readable format within 30 calendar days; and

(b) issue a certificate of deletion confirming secure destruction of Customer Personal Data.

Notwithstanding the foregoing, Provider may retain Customer Personal Data:

(i) as required by applicable law; or

(ii) in accordance with its standard backup or record retention policies; provided that Provider will maintain the confidentiality of such retained data and will not further Process it except as required by applicable law.

Section 8: Audits and Records

8.1. Provider Records

Provider will maintain records of its Processing activities in compliance with Data Protection Laws and will make available to Customer, upon written request, records reasonably necessary to demonstrate compliance with this DPA.

8.2. Third-Party Audit Reports

Provider will make available summary copies of its third-party audit reports and certifications (e.g., SOC 2 Type II, ISO 27001) upon Customer's written request, subject to reasonable confidentiality obligations. Customer may share such reports with relevant government authorities upon their request.

8.3. Customer Audit Rights

Customer may, at its own expense, conduct an audit of reasonable scope and duration, subject to a mutually agreed-upon audit plan. Each audit must:

- Be conducted by an independent third party bound by confidentiality obligations to Provider;
- Be limited in scope to matters reasonably required to assess Provider's compliance with this DPA;
- Occur at a mutually agreed date during Provider's regular business hours;
- Occur no more than once per calendar year (except as required by Data Protection Laws or in connection with a Security Incident);
- Cover only facilities controlled by Provider and restrict findings to Customer Personal Data only.

Audit results are treated as confidential information to the fullest extent permitted by Data Protection Laws.

QUANT

Section 9: Cross-Border Data Transfers

9.1. General Authority to Transfer

Provider (and its Affiliates and Sub-processors) may Process and transfer Customer Personal Data globally as necessary to provide the Cloud Service, subject to the requirements of this Section 9 and Schedule 3. Where a Sub-processor processes data in a country not subject to an adequacy decision, Provider will ensure an appropriate transfer mechanism is in place.

9.2. EU/EEA Transfers — EU Standard Contractual Clauses

Where Customer Personal Data protected by EU GDPR is subject to a Restricted Transfer, the parties incorporate by reference the Standard Contractual Clauses approved by European Commission Decision 2021/914 ("EU SCCs"), as follows:

- Module 2 (Controller to Processor) applies where Customer is a Controller and Provider is a Processor;
- Module 3 (Processor to Processor) applies where Customer is a Processor acting on behalf of a third-party Controller;
- Customer is the "data exporter" and Provider is the "data importer";
- Designated EU Governing Law and courts: Republic of Ireland;
- Schedule 1 of this DPA satisfies Annex I of the EU SCCs; Schedule 2 satisfies Annex II.

9.3. UK Transfers

Where Customer Personal Data protected by UK GDPR is subject to a Restricted Transfer, the EU SCCs (as incorporated above) apply with the modifications specified in the UK International Data Transfer Addendum (ICO, Version B1.0, effective 21 March 2022). Both parties are deemed to have signed the UK Addendum as of the DPA Effective Date.

9.4. Swiss Transfers

Where Customer Personal Data protected by the Swiss FADP is subject to a Restricted Transfer, the EU SCCs apply with the following modifications: (a) the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner (FDPIC); (b) the SCCs are governed by Swiss law; (c) disputes are resolved before Swiss courts; and (d) references to EU GDPR are also deemed to refer to the FADP.

QUANT

Schedule 1:
Subject Matter and Details of Processing

Data Exporter (Customer)

Name	As specified in the Order Form
Contact for Data Protection	As specified in the execution block or Order Form.
Main Address	As specified in the execution block or Order Form.
Role	Controller (or Processor, where applicable).

Data Importer (Provider)

Name	Quant, Inc.
Contact for Data Protection	Provider's Privacy & Security Team - privacy@quant.ai
Main Address	As specified in the Order Form.
Provider Activities	Provider will Process Personal Data as necessary to provide the Services pursuant to the Agreement, as further instructed by Customer in its use of the Services.
Role	Processor.

Details of Processing

Categories of Data Subjects	Customer determines the scope, which may include: • Employees, contractors, and collaborators of Customer; • Customers, prospects, and end users of Customer's products; • Suppliers, subcontractors, and business partners of Customer.
Categories of Personal Data	May include, as determined by Customer: • Identity data: first name, last name, title, employer, position; • Contact data: email address, phone number, business address; • Electronic identifiers: IP addresses, mobile device IDs, session tokens; • Communications data: voice recordings, transcripts, messages (where applicable).
Sensitive Categories	NONE by default. If Customer intends to submit special category data, the parties must agree in writing on additional safeguards prior to any such processing.
Purpose of Processing	Provision of the Cloud Services pursuant to the applicable Order Form and the Agreement.
Duration of Processing	For the duration of the Agreement, unless earlier termination or deletion is requested by Customer in accordance with Section 7 of this DPA.

QUANT

Schedule 2:
Technical and Organizational Measures

For the latest security information, please visit https://quantai.com/security. Provider may update these measures to reflect evolving practices, provided that updates may not be retroactive or materially reduce Provider's overall security obligations during a Subscription Term.

1. Encryption and Pseudonymization

- Full-disk AES-256 encryption required on all employee endpoints.
- Data at rest encrypted using AES-256 via AWS Key Management Service (KMS) with FIPS 140-2 validated HSMs.
- All data in transit protected using TLS 1.2 or higher; email secured with opportunistic TLS.
- Encryption keys rotated at least annually via AWS KMS.
- Hybrid encryption techniques aligned with NIST SP 800-53.

2. Confidentiality, Integrity and Availability

- Role-based access control (RBAC) and multi-factor authentication (MFA) for all systems processing Customer Data.
- Privileged access requires formal approval from designated executives.
- Authentication credentials deactivated promptly upon role change or employment termination.
- Personnel bound by contractual and statutory confidentiality obligations that survive termination.
- Mandatory annual security awareness training covering data privacy, social engineering, and password policies.
- Web application passwords hashed at rest; sessions expire after a configurable inactivity period (default: 30 minutes).

3. Resilience and Recovery

- Geographically distributed data centers via AWS cloud infrastructure.
- Security event logging and real-time alerting across all production systems.
- Incident response procedures aligned with NIST SP 800-61.
- Business continuity and disaster recovery plan informed by periodic risk assessments and threat analysis.
- Annual incident response and DR tests used to update ongoing risk management.

4. Testing and Evaluation

- Regular risk assessments and continuous monitoring via vulnerability scans, penetration testing, and intrusion detection.
- Independent testing team performs vulnerability scanning against internal and external environments.
- Production servers scanned for malware weekly; endpoints protected by continuously updated antivirus software.
- Web application, network segmentation, and interconnections protected by firewalls.
- Provider’s services operate in isolated virtual networks separated from external traffic.

5. User Identification and Authorization

- Commercially reasonable practices to authenticate users accessing information systems.
- MFA required for all remote connections.
- Customers manage their own password complexity, MFA, and SSO/SAML 2.0 settings.

6. Data Protection in Transit

- All Customer-to-Provider communications occur over HTTPS using TLS 1.2+.
- Production environments use logical and physical network segmentation, software-defined networking, and firewalls.
- All internet-facing connections include approved firewall or access control systems.

7. Data Protection at Rest

- Customer Data hosted on AWS; Provider maintains full administrative control over virtual servers.
- AWS KMS manages encryption keys; FIPS 140-2 validated HSMs prevent unauthorized access.
- Multi-tenant Customer Data is logically segregated; cross-tenant access attempts are prevented and logged.
- Antivirus scans run regularly; all personal data access is logged.

8. Physical Security

- Physical access to data hosting facilities documented and managed by AWS.

- Corporate office access restricted to authorized individuals and escorted visitors; zero-trust access model.
- Customers provide no physical media to Provider.
- Digital media access restricted to employees with approved, role-based access.

9. Event Logging and Monitoring

- Event and system access logs monitored and reviewed periodically.
- Audit logs capture timestamp, IP address, user identity, action taken, and requested metadata.
- Central SIEM system and monitoring tools used to detect anomalies and potential threats.
- Customer-facing activity metrics available within the Provider's application.

10. Governance and Certification

- Information Security Management System established in accordance with ISO 27001:2022.
- Sub-processors undergo onboarding due diligence and are required to execute a Data Processing Addendum.
- Three Lines of Defense governance model adopted for transparent compliance management.
- Customers can export Customer Data at any time in standard machine-readable formats.

QUANT

Schedule 3:
Region-Specific Terms

A. California (CCPA/CPRA)

Definitions

The terms "business purpose", "commercial purpose", "personal information", "sell", "service provider", and "share" have the meanings given in the CCPA/CPRA. The definitions of "Data Subject", "Controller", and "Processor" in this DPA include "consumer", "business", and "service provider" as defined under the CCPA, respectively.

Obligations

Customer provides Customer Personal Data to Provider solely for the limited and specific business purposes of providing the Cloud Service and performing under the Agreement. Provider will:

- Comply with all applicable CCPA/CPRA obligations and provide the same level of privacy protection as required by the CCPA;
- Not retain, use, or disclose Customer Personal Data for any purpose other than the specified business purposes, or outside the direct business relationship with Customer;
- Not sell or share Customer Personal Data received under the Agreement;
- Not combine Customer Personal Data with other personal information except as permitted by the CCPA;
- Notify Customer promptly if Provider determines it can no longer meet its CCPA obligations.

B. European Union / EEA (GDPR)

Where Provider Processes Customer Personal Data subject to EU GDPR, the terms of this DPA, including the EU SCCs incorporated by reference in Section 9.2 and Schedule 3, apply. Provider acts as a Processor under Article 28 GDPR. The Designated EU Governing Law and supervisory authority is the Republic of Ireland.

C. United Kingdom (UK GDPR)

Where Provider Processes Customer Personal Data subject to UK GDPR, the terms of this DPA, including the UK International Data Transfer Addendum (ICO, B1.0) incorporated by reference in Section 9.3 and Schedule 3, apply. Provider acts as a Processor as defined under UK GDPR and the UK DPA 2018.

D. Switzerland (FADP)

Where Provider Processes Customer Personal Data subject to the Swiss FADP, the terms of this DPA apply with the modifications set out in Section 9.4 and Schedule 3. The competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner (FDPIC).

Accepted and agreed to as of the date below by the authorized representative of each party:

Provider	Customer
Signature:	Signature:
Full Name:	Full Name:
Title:	Title:
Date:	Date:
Address: 17 State Street, New York, NY 10004, USA	Address:
Privacy Contact: privacy@quant.ai	Privacy Contact: