Data Processing Addendum

Last Updated: May 21st, 2024
Link to Prior Version

This Data Processing Addendum ("DPA") supplements the Terms and Conditions (the "Agreement") between Snorkl, Inc. ("Snorkl," "us," "we") and the entity that is a party to the Agreement ("Organization" or "you"). We may update this Addendum from time to time, and we will provide reasonable notice of any such updates. Any terms not defined in this Addendum shall have the meaning set forth in the Agreement.

1. Definitions

1.1 "Affiliate" means (i) an entity of which a party directly or indirectly owns fifty percent (50%) or more of the stock or other equity interest, (ii) an entity that owns at least fifty percent (50%) or more of the stock or other equity interest of a party, or (iii) an entity which is under common control with a party by having at least fifty percent (50%) or more of the stock or other equity interest of such entity and a party owned by the same person, but such entity shall only be deemed to be an Affiliate so long as such ownership exists.

1.2 "Authorized Sub-Processor" means a third-party who has a need to know or otherwise access Organization's Personal Data to enable Snorkl to perform its obligations under this DPA or the Agreement, and who is either (1) listed in Exhibit B or (2) subsequently authorized under Section 4.2 of this DPA.

1.3 "Snorkl Account Data" means personal data that relates to Snorkl's relationship with Organization, including the names or contact information of individuals authorized by Organization to access Organization's account, including all Business Contact Data. Snorkl Account Data also includes any data Snorkl may need to collect for the purpose of managing its relationship with Organization, identity verification, or as otherwise required by applicable laws and regulations.

1.4 "Snorkl Usage Data" means Service usage data collected and processed by Snorkl in connection with the provision of the Services, including without limitation data used to identify the source and destination of a communication, activity logs, and data used to optimize and maintain performance of the Services, and to investigate and prevent system abuse.

1.5 "Data Exporter" means Organization.

1.6 "Data Importer" means Snorkl.

1.7 "Data Protection Laws" means any applicable laws and regulations in any relevant jurisdiction relating to the use or processing of Personal Data including: (i) the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 ("CCPA"), and (ii) the Virginia Consumer Data Protection Act ("VCDPA") in each case, as updated, amended or replaced from time to time. The terms "Data Subject", "Personal Data", "Personal Data Breach", "processing", "processor," "controller," and "supervisory authority" shall have the meanings set forth in the CCPA and VCDPA.

1.8 "Services" shall have the meaning of providing the Platform as set forth in the Agreement.

2. Relationship of the Parties; Processing of Data

2.1 The parties acknowledge and agree that with regard to the processing of Personal Data, Organization may act either as a controller or processor and, except as expressly set forth in this DPA or the Agreement, Snorkl is a processor. Organization shall, in its use of the Services, at all times process Personal Data, and provide instructions for the processing of Personal Data, in compliance with Data Protection Laws. Organization shall ensure that the processing of Personal Data in accordance with Organization's instructions will not cause Snorkl to be in breach of the Data Protection Laws. Organization is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to Snorkl by or on behalf of Organization, (ii) the means by which Organization acquired any such Personal Data, and (iii) the instructions it provides to Snorkl regarding the processing of such Personal Data. Organization shall not provide or make available to Snorkl any Personal Data in violation of the Agreement or otherwise inappropriate for the nature of the Services, and shall indemnify Snorkl from all claims and losses in connection therewith.

2.2 Snorkl shall not process Personal Data (i) for purposes other than those set forth in the Agreement and/or Exhibit A, (ii) in a manner inconsistent with the terms and conditions set forth in this DPA or any other documented instructions provided by Organization, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Supervisory Authority to which Snorkl is subject; in such a case, Snorkl shall inform the Organization of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest, or (iii) in violation of Data Protection Laws. Organization hereby instructs Snorkl to process Personal Data in accordance with the foregoing and as part of any processing initiated by Organization in its use of the Services.

a. The subject matter, nature, purpose, and duration of this processing, as well as the types of Personal Data collected and categories of Data Subjects, are described in Exhibit A to this DPA.

b. Following completion of the Services, at Organization's choice, Snorkl shall return or delete Organization's Personal Data, unless further storage of such Personal Data is required or authorized by applicable law. If return or destruction is impracticable or prohibited by law, rule or regulation, Snorkl shall take measures to block such Personal Data from any further processing (except to the extent necessary for its continued hosting or processing required by law, rule or regulation) and shall continue to appropriately protect the Personal Data remaining in its possession, custody, or control.

c. CCPA and VCDPA Language. The Parties acknowledge and agree that the processing of personal information or personal data that is subject to the CCPA or VCDPA shall be carried out in accordance with the terms set forth in Exhibit E.

3. Confidentiality

- Snorkl shall ensure that any person it authorizes to process Personal Data has agreed to protect Personal Data in accordance with Snorkl's confidentiality obligations in the Agreement. Organization agrees that Snorkl may disclose Personal Data to its advisers, auditors or other third parties as reasonably required in connection with the performance of its obligations under this DPA, the Agreement, or the provision of Services to Organization.

4. Authorized Sub-Processors

4.1 Organization acknowledges and agrees that Snorkl may (1) engage its Affiliates and the Authorized Sub-Processors to this DPA to access and process Personal Data in connection with the Services and (2) from time to time engage additional third parties for the purpose of providing the Services, including without limitation the processing of Personal Data. By way of this DPA, Organization provides general written authorization to Snorkl to engage sub-processors as necessary to perform the Services.

4.2 A list of Snorkl's current Authorized Sub-Processors (the "List") can be found here. Such List may be updated by Snorkl from time to time. At least ten (10) days before enabling any third party other than existing Authorized Sub-Processors to access or participate in the processing of Personal Data, Snorkl will add such third party to the List and notify Organization via email. Organization may object to such an engagement by informing Snorkl within ten (10) days of receipt of the aforementioned notice by Organization, provided such objection is in writing and based on reasonable grounds relating to data protection. Organization acknowledges that certain sub-processors are essential to providing the Services and that objecting to the use of a sub-processor may prevent Snorkl from offering the Services to Organization.

4.3 If Organization reasonably objects to an engagement in accordance with Section 4.2, and Snorkl cannot provide a commercially reasonable alternative within a reasonable period of time, Organization may discontinue the use of the affected Service by providing written notice to Snorkl. Discontinuation shall not relieve Organization of any fees owed to Snorkl under the Agreement.

4.4 If Organization does not object to the engagement of a third party in accordance with Section 4.2 within ten (10) days of notice by Snorkl, that third party will be deemed an Authorized Sub-Processor for the purposes of this DPA.

4.5 Snorkl will enter into a written agreement with the Authorized Sub-Processor imposing on the Authorized Sub-Processor data protection obligations comparable to those imposed on Snorkl under this DPA with respect to the protection of Personal Data. In case an Authorized Sub-Processor fails to fulfill its data protection obligations under such written agreement with Snorkl, Snorkl will remain liable to Organization for the performance of the Authorized Sub-Processor's obligations under such agreement.

5. Security of Personal Data.

- Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Snorkl shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of processing Personal Data. Exhibit B sets forth additional information about Snorkl's technical and organizational security measures.

6. Rights of Data Subjects

6.1 Snorkl shall, to the extent permitted by law, notify Organization upon receipt of a request by a Data Subject to exercise the Data Subject's right of: access, rectification, erasure, data portability, restriction or cessation of processing, withdrawal of consent to processing, and/or objection to being subject to processing that constitutes automated decision-making (such requests individually and collectively "Data Subject Request(s)"). If Snorkl receives a Data Subject Request in relation to Organization's data, Snorkl will advise the Data Subject to submit their request to Organization and Organization will be responsible for responding to such request, including, where necessary, by using the functionality of the Services. Organization is solely responsible for ensuring that Data Subject Requests for erasure, restriction or cessation of processing, or withdrawal of consent to processing of any Personal Data are communicated to Snorkl, and, if applicable, for ensuring that a record of consent to processing is maintained with respect to each Data Subject.

6.2 Snorkl shall, at the request of the Organization, and taking into account the nature of the processing applicable to any Data Subject Request, apply appropriate technical and organizational measures to assist Organization in complying with Organization's obligation to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, *provided that* (i) Organization is itself unable to respond without Snorkl's assistance and (ii) Snorkl is able to do so in

accordance with all applicable laws, rules, and regulations. Organization shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Snorkl.

7. Snorkl's Role as a Controller. The parties acknowledge and agree that with respect to Business Contact Data and Usage Data, Snorkl is an independent controller, not a joint controller with Organization. Snorkl will process Business Contact Data and Usage Data as a controller (i) to manage the relationship with Organization; (ii) to carry out Snorkl's core business operations, such as accounting, audits, tax preparation and filing and compliance purposes; (iii) to monitor, investigate, prevent and detect fraud, security incidents and other misuse of the Services, and to prevent harm to Organization; (iv) for identity verification purposes; (v) to comply with legal or regulatory obligations applicable to the processing and retention of Personal Data to which Snorkl is subject; and (vi) as otherwise permitted under Data Protection Laws and in accordance with this DPA and the Agreement. Snorkl may also process Snorkl Usage Data as a controller to provide, optimize, and maintain the Services, to the extent permitted by Data Protection Laws. Any processing by Snorkl as a controller shall be in accordance with Snorkl's privacy policy set forth at https://snorkl.app/legal/privacy.

8. **Conflict.** In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the terms of this DPA; (2) the Agreement; and (3) Snorkl's privacy policy. Any claims brought in connection with this DPA will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations set forth in the Agreement.

Exhibit A

Nature and Purpose of Processing: Snorkl will process Organization's Personal Data as necessary to provide the Services under the Agreement, for the purposes specified in the Agreement and this DPA, and in accordance with Organization's instructions as set forth in this DPA. The nature of processing includes, without limitation:

- Receiving data, including collection, accessing, retrieval, recording, and data entry to confirm Services are being provided to the correct individuals
- Holding data, including storage, organization and structuring
- Using data, including analysis, consultation, and testing
- Updating data, including correcting, adaptation, alteration, alignment and combination
- Protecting data, including restricting, encrypting, and security testing
- Sharing data, including disclosure, dissemination, allowing access or otherwise making available
- Returning data to the data exporter or data subject
- Erasing data, including destruction and deletion

Duration of Processing: Snorkl will process Organization's Personal Data as long as required (i) to provide the Platform to Organization under the Agreement; (ii) for Snorkl's legitimate business needs; or (iii) by applicable law or regulation. Snorkl Account Data and Snorkl Usage Data will be processed and stored as set forth in Snorkl's privacy policy.

Categories of Data Subjects: Organization business contacts, Organization's end users, including students.

Categories of Personal Data: Snorkl processes Personal Data contained in Business Contact Data, Usage Data, and any Personal Data provided by Organization as part of the Organization Data (including any Personal Data Organization collects from its end users and processes through its use of the Services) or collected by Snorkl in order to provide the Services or as otherwise set forth in the Agreement or this DPA. Categories of Personal Data include account Information (such as email and name), log data, images, videos, audio, text and other data that is provided by Organization.

Sensitive Data or Special Categories of Data: None

Exhibit B

Description of the Technical and Organizational Security Measures implemented by the Data Importer

Technical and Organizational Security Measure	Details
Measures of pseudonymisation and encryption of personal data	All data is encrypted at rest and in transit. All sub processors of data also encrypt data at rest and in transit.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	System Resilience Snorkl backend is designed in different components which are independently scalable and redundant. For web servers, we can start additional web servers elastically. For the database, we have hot standby (replicas) in different active zones in the primary region and secondary region, which can be promoted to masters. Snorkl leverage SQS for asynchronous workflows, which leverage multiple active zones to achieve high availability. Data backup and restoration Snorkl backs up and recovers from system failure. Snorkl performs data backup daily for the last 7 days.
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	Database is backed up daily in the last 7 days. Time to recovery once issues are detected: 5 minutes to restart/failover same region database master.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	Snorkl works with the iKeepSafe Safe Harbor program, which uses a combination of manual and technical assessments to determine fitness of our security systems. Initial assessment completed Q2 2024. Snorkl also regularly uses the NIST CSF 1.1 framework to assess and improve its cybersecurity measures.
Measures for user identification and authorization	All Snorkl devices and websites support SSO and multi-factor authentication. These controls ensure that access to any systems is limited to only authorized users. Snorkl uses single sign on and 2FA authentication to authenticate customers.
Measures for the protection of data during transmission	All data is encrypted at rest and in transit. Data transfer is done via secure sub-processors.
Measures for the protection of data during storage	Snorkl's data is encrypted at rest by its sub processors (AWS and Render).
Measures for ensuring events logging	Snorkl uses Datadog for event monitoring and reporting. All logs are stored only for 15 days and personal identifiable data are anonymized and masked..
Measures for ensuring system configuration, including default configuration	Snorkl actively monitors vulnerabilities in Snorkl's cloud environment and software libraries. Security patches are applied within 30 days of identifying vulnerabilities. All Snorkl's infrastructure (databases, cache store, etc) automatically applies security patches through Render.
Measures for internal IT and IT security governance and management	Snorkl uses NIST CSF to assess and make choices about internal IT and IT security governance and management. Snorkl limits users' access to only tools and data required for their roles. This ensures that users are only able to access the relevant data for their work and roles.
Measures for certification/assurance of processes and products	Snorkl is certified by iKeepSafe Safe Harbor program. They conduct security audits at least 3 times per year.
Measures for ensuring data minimisation	Snorkl collects only the relevant information from users to use the platform.

	For educators, that includes their classes and the assignments they give to students. For students, that includes recordings of their voice & work on a digital whiteboard in response to teacher-created assignments. Students' faces and physical environment are never recorded.
Measures for ensuring data quality	Snorkl performs data standardization for all ingested data to fit into Snorkl's domain model. Any failure for such normalization will trigger alerts and is resolved by on-call engineers. Snorkl also uses analytics to profile data to identify outliers in data distribution.
Measures for ensuring limited data retention	We retain Personal Data about you for as long as necessary to provide you with our Platform or to perform our business or commercial purposes for collecting your Personal Data. When establishing a retention period for specific categories of data, we consider who we collected the data from, our need for the Personal Data, why we collected the Personal Data, and the sensitivity of the Personal Data. In some cases we retain Personal Data for longer, if doing so is necessary to comply with our legal obligations, resolve disputes or collect fees owed, or is otherwise permitted or required by applicable law, rule or regulation.
Measures for ensuring accountability	Snorkl is in the process of implementing an IT training program for its employees. These trainings will include but are not limited to information security, information security roles and responsibilities, physical security, data privacy, operations security, asset management, access control, data management, risk management, third-party management, cryptography, incident response, business continuity and disaster recovery, anti-corruption, and human resource security policies.
Measures for allowing data portability and ensuring erasure	Data portability between Snorkl and client is through Snorkl application and cloud storage buckets (S3). Data is stored in Snorkl internal formats unless Snorkl is contracted to provide specific format data to clients.
Technical and organizational measures of sub-processors	Snorkl's services agreements with all Sub Processors require that such Sub Processors adhere to commercially reasonable industry standards and security practices with respect to its handling of data, and employ compliant data handling practices required under applicable law.
Measures for addressing and responding to a data breach	In the event of a personal data breach we shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. We will also notify Organizations without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

Exhibit C

United States Privacy Law Exhibit

This United States Privacy Law Exhibit ("Exhibit") supplements the DPA and includes additional information required by the CCPA and the VCDPA, in each case, as updated, amended or replaced from time to time. Any terms not defined in this Exhibit shall have the meanings set forth in the DPA and/or the Agreement.

A. CALIFORNIA

1. Definitions

1.1 For purposes of this Section A, the terms "Business," "Business Purpose," "Commercial Purpose," "Consumer," "Personal Information," "Processing," "Sell," "Service Provider," "Share," and "Verifiable Consumer Request" shall have the meanings set forth in the CCPA.

1.2 All references to "Personal Data," "Controller," "Processor," and "Data Subject" in the DPA shall be deemed to be references to "Personal Information," "Business," "Service Provider," and "Consumer," respectively, as defined in the CCPA.

2. Obligations

2.1 Except with respect to Snorkl Account Data and Snorkl Usage Data (as defined in the DPA), the parties acknowledge and agree that Snorkl is a Service Provider for the purposes of the CCPA (to the extent it applies) and Snorkl is receiving Personal Information from Organization in order to provide the Services pursuant to the Agreement, which constitutes a Business Purpose.

2.2 Organization shall disclose Personal Information to Snorkl only for the limited and specified purposes described in Exhibit A to this DPA.

2.3 Snorkl shall not Sell or Share Personal Information provided by Organization under the Agreement.

2.4 Snorkl shall not retain, use, or disclose Personal Information provided by Organization pursuant to the Agreement for any purpose, including a Commercial Purpose, other than as necessary for the specific purpose of performing the Services for Organization pursuant to the Agreement, or as otherwise set forth in the Agreement or as permitted by the CCPA.

2.5 Snorkl shall not retain, use, or disclose Personal Information provided by Organization pursuant to the Agreement outside of the direct business relationship between Snorkl and Organization, except where and to the extent permitted by the CCPA.

2.6 Snorkl shall notify Organization if it makes a determination that it can no longer meet its obligations under the CCPA.

2.7 Snorkl will not combine Personal Information received from, or on behalf of, Organization with Personal Information that it receives from, or on behalf of, another party, or that it collects from its own interaction with the Consumer.

2.8 Snorkl shall comply with all obligations applicable to Service Providers under the CCPA, including by providing Personal Information provided by Organization under the Agreement the level of privacy protection required by CCPA.

2.9 Snorkl shall only engage a new sub-processor to assist Snorkl in providing the Services to Organization under the Agreement in accordance with Section 4.1 of the DPA, including, without limitation, by: (i) notifying Organization of such engagement via the notification mechanism described in Section 4.1 of the DPA at least ten (10) days before enabling a new Sub-Processor; and (ii) entering into a written contract with the sub-processor requiring sub-processor to observe all of the applicable requirements set forth in the CCPA.

3. Consumer Rights

3.1 Snorkl shall assist Organization in responding to Verifiable Consumer Requests to exercise the Consumer's rights under the CCPA as set forth in Section 7 of the DPA.

4. Audit Rights

4.1 To the extent required by CCPA, Snorkl shall allow Organization to conduct inspections or audits in accordance with the DPA.

B. VIRGINIA

1. Definitions

1.1 For purposes of this Section B, the terms "Consumer," "Controller," "Personal data," "Processing," and "Processor" shall have the meanings set forth in the VCDPA.

1.2 All references to "Data Subject" in this DPA shall be deemed to be references to "Consumer" as defined in the VCDPA.

2. Obligations

2.1 Except with respect to Snorkl Account Data and Snorkl Usage Data (as defined in the DPA), the parties acknowledge and agree that Organization is a Controller and Snorkl is a Processor for the purposes of the VCDPA (to extent it applies).

2.2 The nature, purpose, and duration of Processing, as well as the types of Personal Data and categories of Consumers are described in Exhibit A to this DPA.

2.3 Snorkl shall adhere to Organization's instructions with respect to the Processing of Organization Personal Data and shall assist Organization in meeting its obligations under the VCDPA by:

2.3.1 Assisting Organization in responding to Consumer rights requests under the VCDPA as set forth in Section 7 of the DPA;

2.3.2 Complying with Section 5 ("Security of Personal Data") of the DPA with respect to Personal Data provided by Organization;

2.3.3 In the event of a Personal Data Breach, providing information sufficient to enable Organization to meet its obligations pursuant to Va. Code § 18.2-186.6; and

2.3.4 Providing information sufficient to enable Organization to conduct and document data protection assessments to the extent required by VCDPA.

2.4 Snorkl shall maintain the confidentiality of Personal Data provided by Organization and require that each person processing such Personal Data be subject to a duty of confidentiality with respect to such Processing;

2.5 Upon Organization's written request, Snorkl shall delete or return all Personal Data provided by Organization in accordance with Section 2.4 of the DPA, unless retention of such Personal Data is required or authorized by law or the DPA and/or Agreement.

2.6 In the event that Snorkl engages a new sub-processor to assist Snorkl in providing the Services to Organization under the Agreement, Snorkl shall enter into a written contract with the sub-processor requiring sub-processor to observe all of the applicable requirements of a Processor set forth in the VCDPA.

3. **Audit Rights**

3.1 Upon Organization's written request at reasonable intervals, Snorkl shall, (i) make available to Organization all information in its possession that is reasonably necessary to demonstrate Snorkl's compliance with its obligations under the VCDPA; and (ii) allow and cooperate with reasonable inspections or audits as required under the VCDPA.