Data Processing Addendum

Last Updated: November 3, 2023

This Data Processing Addendum ("**DPA**") supplements the Keyboard Logic Customer Agreement available at https://www.keyboardlogic.io/legal/customer-agreement, as updated from time to time between Customer and Keyboard Logic, or other agreement between Customer and Keyboard Logic governing Customer's use of the Services (the "**Agreement**"). This DPA is an agreement between you and the entity you represent ("**Customer**", "**you**" or "**your**") and Keyboard Logic LLC and its affiliates under the Agreement (together "**Keyboard Logic**"). Unless otherwise defined in this DPA or in the Agreement, all capitalized terms used in this DPA will have the meanings given to them in Section 16 of this DPA.

1. **Data Processing**.
   - 1.1. **Scope and Roles**. This DPA applies when Customer Data is processed by Keyboard Logic. In this context, Keyboard Logic will act as processor to Customer, who can act either as controller or processor of Customer Data.
   - 1.2. **Customer Controls**. Customer can use the Service Controls to assist it with its obligations under Applicable Data Protection Law, including its obligations to respond to requests from data subjects. Taking into account the nature of the processing, Customer agrees that it is unlikely that Keyboard Logic would become aware that Customer Data transferred under the Standard Contractual Clauses is inaccurate or outdated. Nonetheless, if Keyboard Logic becomes aware that Customer Data transferred under the Standard Contractual Clauses is inaccurate or outdated, it will inform Customer without undue delay. Keyboard Logic will cooperate with Customer to erase or rectify inaccurate or outdated Customer Data transferred under the Standard Contractual Clauses by providing the Service Controls that Customer can use to erase or rectify Customer Data.
   - 1.3. **Details of Data Processing**.
     - 1.3.1. **Subject matter**. The subject matter of the data processing under this DPA is Customer Data.
     - 1.3.2. **Duration**. As between Keyboard Logic and Customer, the duration of the data processing under this DPA is determined by Customer.
     - 1.3.3. **Purpose**. The purpose of the data processing under this DPA is the provision of the Services initiated by Customer from time to time.
     - 1.3.4. **Nature of the processing**. Compute, storage and such other Services as described in the Documentation and initiated by Customer from time to time.
     - 1.3.5. **Type of Customer Data**. Customer Data uploaded to the Services under Customer's Keyboard Logic accounts.
     - 1.3.6. **Categories of data subjects**. The data subjects could include Customer's customers, employees, suppliers and End Users.
   - 1.4. **Compliance with Laws**. Each party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this DPA, including Applicable Data Protection Law.

2. **Customer Instructions**. The parties agree that this DPA and the Agreement (including Customer providing instructions via configuration tools such as user interfaces and APIs made available by Keyboard Logic for the Services) constitute Customer's documented instructions regarding Keyboard Logic's processing of Customer Data ("**Documented Instructions**"). Keyboard Logic will process Customer Data only in accordance with Documented Instructions (which if Customer is acting as a processor, could be based on the instructions of its controllers). Additional instructions outside the scope of the Documented Instructions (if any) require prior written agreement between Keyboard Logic and Customer, including agreement on any additional fees payable by Customer to Keyboard Logic for carrying out such instructions. Customer is entitled to terminate this DPA and the Agreement if Keyboard Logic declines to follow instructions requested by Customer that are outside the scope of, or changed from, those given or agreed to be given in this DPA. Taking into account the nature of the processing, Customer agrees that it is unlikely Keyboard Logic can form an opinion on whether Documented Instructions infringe Applicable Data Protection Law. If Keyboard Logic forms such an opinion, it will immediately inform Customer, in which case, Customer is entitled to withdraw or modify its Documented Instructions.
3. **Confidentiality of Customer Data**. Keyboard Logic will not access or use, or disclose to any third party, any Customer Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order). If a governmental body sends Keyboard Logic a demand for Customer Data, Keyboard Logic will attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, Keyboard Logic may provide Customer's basic contact information to the governmental body. If compelled to disclose Customer Data to a governmental body, then Keyboard Logic will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Keyboard Logic is legally prohibited from doing so.
4. **Confidentiality Obligations of Keyboard Logic Personnel**. Keyboard Logic restricts its personnel from processing Customer Data without authorization by Keyboard Logic as described in the Security Standards. Keyboard Logic imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.
5. **Security of Data Processing**.
   5.1. Keyboard Logic has implemented and will maintain the technical and organizational measures for the Keyboard Logic Network as described in the Security Standards and this Section. In particular, Keyboard Logic has implemented and will maintain the following technical and organizational measures:
      5.1.1. security of the Keyboard Logic Network as set out in Section 1.1 of the Security Standards;
      5.1.2. physical security of the facilities as set out in Section 1.2 of the Security Standards;
      5.1.3. measures to control access rights for authorized personnel to the Keyboard Logic Network as set out in Section 1.3 of the Security Standards; and

5.1.4. processes for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures implemented by Keyboard Logic as described in Section 2 of the Security Standards.

6. **Sub-processing**.

6.1. **Authorized Sub-processors**. Customer provides general authorization to Keyboard Logic's use of sub-processors to provide processing activities on Customer Data on behalf of Customer ("**Sub-processors**") in accordance with this Section. The Keyboard Logic website (currently posted at https://keyboardlogic.io/legal/sub-processors) lists Sub-processors that are currently engaged by Keyboard Logic. At least 15 days before Keyboard Logic engages a Sub-processor, Keyboard Logic will update the applicable website. To object to a Sub-processor, Customer can:

6.1.1. terminate the Agreement pursuant to its terms; or

6.1.2. cease using the Service for which Keyboard Logic has engaged the Sub-processor.

6.2. **Sub-processor Obligations**. Where Keyboard Logic authorizes a Sub-processor as described in Section 6.1:

6.2.1. Keyboard Logic will restrict the Sub-processor's access to Customer Data only to what is necessary to provide or maintain the Services in accordance with the Documentation, and Keyboard Logic will prohibit the Sub-processor from accessing Customer Data for any other purpose;

6.2.2. Keyboard Logic will enter into a written agreement with the Sub-processor and, to the extent that the Sub-processor performs the same data processing services provided by Keyboard Logic under this DPA, Keyboard Logic will impose on the Sub-processor the same contractual obligations that Keyboard Logic has under this DPA; and

6.2.3. Keyboard Logic will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause Keyboard Logic to breach any of Keyboard Logic's obligations under this DPA.

7. **Keyboard Logic Assistance with Data Subject Requests**. Taking into account the nature of the processing, the Service Controls are the technical and organizational measures by which Keyboard Logic will assist Customer in fulfilling Customer's obligations to respond to data subjects' requests under Applicable Data Protection Law. If a data subject makes a request to Keyboard Logic, Keyboard Logic will promptly forward such request to Customer once Keyboard Logic has identified that the request is from a data subject for whom Customer is responsible. Customer authorizes on its behalf, and on behalf of its controllers when Customer is acting as a processor, Keyboard Logic to respond to any data subject who makes a request to Keyboard Logic, to confirm that Keyboard Logic has forwarded the request to Customer. The parties agree that Customer's use of the Service Controls and Keyboard Logic forwarding data subjects' requests to Customer in accordance with this Section, represent the scope and extent of Customer's required assistance.

8. **Security Incident Notification**.

8.1. **Security Incident**. Keyboard Logic will

8.1.1. notify Customer of a Security Incident without undue delay after becoming aware of the Security Incident, and

8.1.2. take appropriate measures to address the Security Incident, including measures to mitigate any adverse effects resulting from the Security Incident.

8.2. **Keyboard Logic Assistance**. To enable Customer to notify a Security Incident to supervisory authorities or data subjects (as applicable), Keyboard Logic will cooperate with and assist Customer by including in the notification under Section 8.1.1 such information about the Security Incident as Keyboard Logic is able to disclose to Customer, taking into account the nature of the processing, the information available to Keyboard Logic, and any restrictions on disclosing the information, such as confidentiality. Taking into account the nature of the processing, Customer agrees that it is best able to determine the likely consequences of a Security Incident.

8.3. **Unsuccessful Security Incidents**. Customer agrees that:

8.3.1. an unsuccessful Security Incident will not be subject to this Section 8. An unsuccessful Security Incident is one that results in no unauthorized access to Customer Data or to any of Keyboard Logic's equipment or facilities storing Customer Data, and could include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents; and

8.3.2. Keyboard Logic's obligation to report or respond to a Security Incident under this Section 8 is not and will not be construed as an acknowledgement by Keyboard Logic of any fault or liability of Keyboard Logic with respect to the Security Incident.

8.4. **Communication**. Notification(s) of Security Incidents, if any, will be delivered to one or more of Customer's administrators by any means Keyboard Logic selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information for their Keyboard Logic account and secure transmission at all times.

8.5. **Notification Obligations**. If Keyboard Logic notifies Customer of a Security Incident, or Customer otherwise becomes aware of any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data, Customer will be responsible for

8.5.1. determining if there is any resulting notification or other obligation under Applicable Data Protection Law and

8.5.2. taking necessary action to comply with those obligations. This does not limit Keyboard Logic's obligations under this Section 8.

9. **Keyboard Logic Audit Rights**.

9.1. **Audit**. Keyboard Logic shall make available to the Customer, on Customer's written request and provided that the parties have an applicable NDA in place, all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, in relation to the processing of the Customer Data. All information provided under this Section 9 will be considered Keyboard Logic's Confidential Information. Information and audit rights of the Customer only arise under this Section 9 to the extent that the Agreement does not

otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

9.2. **Privacy Impact Assessment and Prior Consultation**. Taking into account the nature of the processing and the information available to Keyboard Logic, Keyboard Logic will assist Customer in complying with Customer's obligations in respect of data protection impact assessments and prior consultation, by providing the information Keyboard Logic makes available under this Section 9.

10. **Customer Audits**. Customer chooses to conduct any audit, including any inspection, it has the right to request or mandate on its own behalf, and on behalf of its controllers when Customer is acting as a processor, under Applicable Data Protection Law or the Standard Contractual Clauses, by instructing Keyboard Logic to carry out the audit described in Section 9. If Customer wishes to change this instruction regarding the audit, then Customer has the right to request a change to this instruction by sending Keyboard Logic written notice as provided for in the Agreement. If Keyboard Logic declines to follow any instruction requested by Customer regarding audits, including inspections, Customer is entitled to terminate the Agreement in accordance with its terms.
11. **Transfers of Personal Data**.
    11.1. **Application of Standard Contractual Clauses**. Subject to Section 11.2, the Standard Contractual Clauses will only apply to Customer Data subject to the GDPR that is transferred, either directly or via onward transfer, to any Third Country (each a "**Data Transfer**").
        11.1.1. When Customer is acting as a controller, the Controller-to-Processor Clauses will apply to a Data Transfer.
        11.1.2. When Customer is acting as a processor, the Processor-to-Processor Clauses will apply to a Data Transfer. Taking into account the nature of the processing, Customer agrees that it is unlikely that Keyboard Logic will know the identity of Customer's controllers because Keyboard Logic has no direct relationship with Customer's controllers and therefore, Customer will fulfil Keyboard Logic's obligations to Customer's controllers under the Processor-to-Processor Clauses.
    11.2. **Alternative Transfer Mechanism**. The Standard Contractual Clauses will not apply to a Data Transfer if Keyboard Logic has adopted Binding Corporate Rules for Processors or an alternative recognized compliance standard for lawful Data Transfers.
12. **Termination of the DPA**. This DPA will continue in force until the termination of the Agreement (the "**Termination Date**").
13. **Return or Deletion of Customer Data**. At any time up to the Termination Date, and for 90 days following the Termination Date, subject to the terms and conditions of the Agreement, Keyboard Logic will return or delete Customer Data when Customer uses the Service Controls to request such return or deletion. No later than the end of this 90-day period, Customer will close all Keyboard Logic accounts containing Customer Data.
14. **Duties to Inform**. Where Customer Data becomes subject to confiscation during bankruptcy or insolvency proceedings, or similar measures by third parties while being processed by Keyboard Logic, Keyboard Logic will inform Customer without undue delay. Keyboard Logic will, without undue delay, notify all relevant parties in such action (for example, creditors,

bankruptcy trustee) that any Customer Data subjected to those proceedings is Customer's property and area of responsibility and that Customer Data is at Customer's sole disposition.

15. **Entire Agreement; Conflict**. This DPA incorporates the Standard Contractual Clauses by reference. Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between the Agreement and this DPA, the terms of this DPA will control, except that the Service Terms will control over this DPA. Nothing in this document varies or modifies the Standard Contractual Clauses.
16. **Definitions**. Unless otherwise defined in the Agreement, all capitalized terms used in this DPA will have the meanings given to them below:
    16.1. "**API**" means an application program interface.
    16.2. "**Applicable Data Protection Law**" means all laws and regulations applicable to and binding on the processing of Customer Data by a party, including, as applicable, the GDPR.
    16.3. "**Keyboard Logic Network**" means the servers, networking equipment, and host software systems (for example, virtual firewalls) that are within Keyboard Logic's control and are used to provide the Services.
    16.4. "**Binding Corporate Rules**" has the meaning given to it in the GDPR.
    16.5. "**controller**" has the meaning given to it in the GDPR.
    16.6. "**Controller-to-Processor Clauses**" means the standard contractual clauses between controllers and processors for Data Transfers, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and currently located at https://keyboardlogic.io/legal/controller-to-processor-transfers.
    16.7. "**Customer Data**" means the Personal Data that is uploaded to the Services under Customer's Keyboard Logic accounts.
    16.8. "**Documentation**" means the then-current documentation for the Services located on the Keyboard Logic Site (and any successor locations designated by Keyboard Logic) and/or provided with the Services.
    16.9. "**EEA**" means the European Economic Area.
    16.10. "**GDPR**" means Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
    16.11. "**Personal Data**" means personal data, personal information, personally identifiable information or other equivalent term (each as defined in Applicable Data Protection Law).
    16.12. "**processing**" has the meaning given to it in the GDPR and "**process**", "**processes**" and "**processed**" will be interpreted accordingly.
    16.13. "**processor**" has the meaning given to it in the GDPR.
    16.14. "**Processor-to-Processor Clauses**" means the standard contractual clauses between processors for Data Transfers, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and currently located at https://keyboardlogic.io/legal/processor-to-processor-transfers.

16.15. "**Security Incident**" means a breach of Keyboard Logic's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data.
16.16. "**Security Standards**" means the security standards attached to this DPA as Annex 1.
16.17. "**Service Controls**" means the controls, including security features and functionalities, that the Services provide, as described in the Documentation.
16.18. "**Standard Contractual Clauses**" means (i) the Controller-to-Processor Clauses, or (ii) the Processor-to-Processor Clauses, as applicable in accordance with Sections 11.1.1 and 11.1.2.
16.19. "**Third Country**" means a country outside the EEA not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR).

Annex 1: Security Standards

1. **Information Security Program**. Keyboard Logic will maintain an information security program designed to
   1.1. secure Customer Data against accidental or unlawful loss, access, or disclosure,
   1.2. identify reasonably foreseeable risks to the security and availability of the Keyboard Logic Network, and
   1.3. minimize security risks to the Keyboard Logic Network, including through regular risk assessment and testing. Keyboard Logic's information security program will include the following measures:
      1.3.1. **Access Controls**. Keyboard Logic will make the Keyboard Logic Network accessible only to authorized personnel, and only as necessary to maintain and provide the Services. Keyboard Logic will maintain access controls and policies to manage authorizations for access to the Keyboard Logic Network from each network connection and user, including through the use of firewalls or functionally equivalent technology and authentication controls. Keyboard Logic will maintain access controls designed to restrict unauthorized access to data.
      1.3.2. **Restricted User Access**. Keyboard Logic will provision and restrict user access to the Keyboard Logic Network in accordance with least privilege principles based on personnel job functions, require at least annually review of Keyboard Logic Network access privileges and, where necessary, revoke Keyboard Logic Network access privileges in a timely manner.
2. **Continued Evaluation**. Keyboard Logic will conduct periodic reviews of the information security program for the Keyboard Logic Network. Keyboard Logic will update or alter its information security program as necessary to respond to new security risks and to take advantage of new technologies.