Data Processing Agreement

This Data Processing Agreement (this "**DPA**") is by and between KeyStrike Inc., a software company whose address is at 8 The Green, Suite # 1128, Dover, DE 19901, Kent County, Delaware USA (the "**Data Processor**"), and the corporation, limited liability company, partnership, sole proprietorship, other business entity or individual executing this DPA (the "**Company**"). The Data Processor and the Company are sometimes referred to herein collectively as the "Parties" and individually as a "Party".

The Parties have agreed to enter into this DPA in consideration of their mutual obligations and commitments hereunder.

WHEREAS

(A) The Company acts as a Data Controller.
(B) The Company wishes to subcontract certain services which imply the processing of personal data, to the Data Processor.
(C) The Parties seek to implement a data processing agreement that complies with the requirements of the General Data Protection Regulation (EU) no 2016/679 ("**GDPR**").

1. Purpose and Effect of this DPA

1.1. This DPA reflects the Parties' agreement with respect to the processing of personal data by the Data Processor on behalf of the Company in connection with the Data Processor's services under the Hybrid Cloud

Subscription Terms of Service and License Agreement ("**the ToS and LA**") between the Company and the Data Processor.

1.2. By signing this DPA with electronic means, such as by acceptance box, the Company agrees to be bound by this DPA as of the date of signature (the "**Effective Date**").

2. Processing Activities by the Data Processor

2.1. On behalf of the Company, the Data Processor is permitted to process the personal data necessary to provide the services described under the ToS and LA and otherwise for the processing activities described below.
2.2. The processing of personal data is for the purposes of the following Processing Activities:
2.2.1. Provide, maintain, develop and improve the services of the Data Processor described in the ToS and LA as well as for security purposes, fraud prevention, marketing and promotional purposes;
2.2.2. Disclosure in accordance with the ToS and LA and this DPA and/or as compelled by applicable laws;
2.3. The Data Processor is permitted to process the following types of Personal Data, as further described in the Data Processor's Privacy Policy:
(i) Contact information of Administrator (e.g. name and email address)
(ii) Device information (e.g. Device ID, Device name, operating system, IP address)
(iii)User information (e.g. Username and user ID)
(iv)Usage data e.g.:

- Device event information (such as system activity, error reports and hardware settings)
- Activity of users (Such as the date/time stamps associated with usage and how the service is used))
- Log data, including device information, browser type, URLs and settings etc.

2.4. The Data Processor is permitted to process the following categories of Data Subjects

- Employees of Customers.

3. Obligations of the Data Processor

3.1. The Data Processor shall:

3.1.1. Comply with all applicable data protection law in the processing of Company Personal Data; and

3.1.2. Only process Company Personal Data in accordance with this DPA;

3.1.3. Only process Company Personal Data in accordance with the Company's documented instructions, which are identified in this DPA. In cases where the Data Processor believes that the Company's instructions are not compatible with the GDPR or other relevant legal provisions concerning the processing of personal data, he must notify the Company without delay;

3.1.4. Ensure that the employees who have access to personal data in connection with the execution of the contract have signed a confidentiality statement or are bound by the law to confidentiality and that they receive appropriate training in the protection of personal data;

3.1.5. Make sure that devices, products, programmes and services are

designed with built-in and default personal protection as a guiding principle.

4. Use of Sub-Processors

4.1. As a general authorisation of the Company, the Data Processor is entitled to engage another processor (hereinafter referred to as "**Sub-Processor**").
4.2. The Data Processor's use of Sub-Processors is based on written agreements that ensure the continuation of at least the same level of protection as the level specified in this DPA.
4.3. At the acceptance of this DPA, the Company simultaneously authorises the Data Processor's use of the Sub-Processors listed below:

- Google Cloud Platform – for cloud computing services
- Sendgrid – for emailing
- Zendesk – for helpdesk
- Google Analytics – for web and mobile analytics

4.4. As a consequence of the general authorisation, cf. section 4.1., the Data Processor shall inform the Company of any intended changes concerning the addition or replacement of Sub-Processors with a notice of 14 days, thereby giving the Company the opportunity to object to such changes within 10 days. In case of an objection from the Company, which the Data Processor cannot meet the content of, the services of the Data Processor, as described in the ToS and LA, will be considered terminated by the Company.
4.5. When using a Sub-Processor, the Data Processor shall ensure that the

Sub-Processor is subject to the same data protection obligations as those specified in this DPA on the basis of a contract or other legal document under EU law or the national law of the Member States, in particular providing the necessary guarantees that the Sub-Processor will implement the appropriate technical and organisational measures in such a way that the processing meets the requirements of the GDPR.
4.6. If the Sub-Processor does not fulfil its data protection obligations, the Data Processor shall remain liable to the Company as regards the fulfilment of the obligations of the Sub-Processor, as required by the GDPR.

5. Providing information of the Processing Activities

5.1. The Company is responsible for providing the data subject with information about the processing activity before or as soon as processing begins, in accordance with the provisions of the GDPR on information that must be provided to the data subject, cf. i.a. Articles 13 and 14.

6. Data Subject Rights

6.1. Taking into account the nature of the processing, the Data Processor shall assist the Company by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company's obligations, as reasonably understood by the Company, to respond to requests to exercise Data Subject rights under the GDPR.
6.2. Data Processor shall:
6.2.1. Promptly notify the Company if it receives a request from a Data

Subject under any data protection law in respect of the Company Personal Data; and

6.2.2. Ensure that it does not respond to that request except on the documented instructions of the Company or as required by applicable laws to which the Data Processor is subject, in which case the Data Processor shall to the extent permitted by applicable laws inform the Company of that legal requirement before responding to the request.

7. Security

7.1. 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, the Data Processor shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

7.2. The Company Personal Data in transit over public networks between the Company and the Data Processor, or between the Data Processor data centres, is encrypted by default. Company Personal Data is encrypted at rest in Google Cloud Platform, using Google encryption keys. The Company Personal Data is only accessible through bastion host, designed and configured to withstand attacks from external networks.

7.3. The Data Processor employs least privilege access mechanisms to control access to Company Personal Data. Role-based access controls are employed to ensure that access to Company Personal Data required for service operations is for an appropriate purpose and approved with

management oversight.
7.4. Third party penetration testing of the Data Processor's systems is carried out yearly in order to identify security vulnerabilities and mitigate risk.
7.5. The Data Processor employs a point-in-time restore of data and exports daily backups from log-storage to a different region.
7.6. In assessing the appropriate level of security, the Data Processor shall take account in particular of the risks that are presented by the processing.

8. Personal Data Breach

8.1. The Data Processor shall notify the Company without undue delay upon Data Processor becoming aware of a Personal Data Breach affecting Company Personal Data, providing the Company with sufficient information to allow the Company to meet any obligations to report or inform Data Subjects of the Personal Data Breach under applicable data protection laws. The notification must be accompanied by the documents or data that are necessary for the Company to report the breach to the relevant supervisory authority.
8.2. The Data Processor shall cooperate with the Company and take reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

9. Data Protection Impact Assessment and Prior Consultation

9.1. The Data Processor shall provide reasonable assistance to the Company with any data protection impact assessments, and prior consultations with competent data privacy authorities, which the Company reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other applicable data protection law, in each case solely in relation to processing of Company Personal Data, and taking into account the nature of the processing and information available to the Data Processor.

10. Audit rights

10.1 Subject to this section 11, the Data Processor shall make available to the Company on request all information necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, including inspections, by the Company or an auditor mandated by the Company in relation to the processing of the Company Personal Data by the Data Processor.

10.2. The Company and the Data Processor shall mutually decide the procedures of inspections, the type of audit report and which authorised, independent third party shall carry out the audit and/or the inspection.

10.3. Information and audit rights of the Company only arise under section 11.1 to the extent that the DPA does not otherwise give them information and audit rights meeting the relevant requirements of data protection law.

10.4. The Company shall incur all costs related to the audit or inspection of the Data Processor's compliance with this DPA as described in this section 11.

11. Data Transfer

11.1. Company Personal Data may only be transferred to, stored or processed in a geographic location in accordance with this DPA. Taking into account the safeguards stipulated in this DPA, the Company appoints the Data Processor to transfer Company Personal Data to the United States or any other country in which the Data Processor or its Sub-Processors operate, store and process the Company Personal Data for the purposes described in section 2 of this DPA.
11.2. The Data Processor will abide by the requirements of the EU/EEA data protection law regarding the collection, use, transfer, retention and other processing of the Company Personal Data from the EU/EEA. All transfers of the Company Personal Data to a third country will be subject to adequate protection in accordance with the GDPR.
11.3. The Data Processor is certified under the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework and the Swiss-U.S. Data Privacy Framework ("DPF") as administered by the U.S. Department of Commerce. The Data Processor adheres to the principles and obligations set out in these frameworks with respect to the processing of personal data transferred from the EU/EEA, the UK and Switzerland to the United States. The Data Processor's certification status is publicly available on the official Data Privacy Framework List maintained

by the U.S. Department of Commerce and is further described in its Privacy Policy.

12. Term

12.1. By signing this DPA with electronic means, such as by acceptance box, the Company agrees to be bound by this DPA as of the Effective Date. This DPA will remain in force until the termination of the processing of Company Personal Data and the erasure of the Company Personal Data by the Data Processor and any Sub-Processors.

13. Handling of Data After the Termination of the DPA

13.1. At the termination of this DPA, the Data Processor shall be under obligation, at the Company's discretion, to erase or return all the Personal Data to the Company and to erase existing copies unless EU law or national law requires the storage of the Personal Data.
13.2. The Data Processor is entitled to erase Company Personal Data if the Company has not requested returning of the Personal Data within 30 days after the termination of this DPA.

14. Governing Law and Jurisdiction

14.1 This DPA is governed by the internal laws of the State of Delaware, United States.
14.2 Any dispute arising in connection with this DPA, which the Parties will not be able to resolve amicably, will be submitted to the exclusive

jurisdiction of the courts of the State of Delaware, United States, so long as other relevant recourse mechanisms, e.g. under the DPF, have been fully tested.