DATA PROCESSING ADDENDUM
(with Standard Contractual Clauses)

This Data Processing Addendum (**DPA**) is entered into between the Customer and SearchStax, Inc., a Delaware corporation (**SearchStax**), and Customer, and is incorporated into and governed by the terms of the Subscription Services Agreement (**Agreement**) between the parties.

DEFINITIONS. Any capitalised term not defined in this DPA will have the meaning given to it in the Agreement (defined below).

- **Affiliate** *means* any entity that directly or indirectly controls, is controlled by, or is under common control of a party. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of a party.

- **Agreement** means the Subscription Services Agreement between Customer and SearchStax for the provision of the Services.

- **CCPA** *means* the California Consumer Privacy Act of 2018, along with its regulations, and as amended**.**

- **Controller** *means* Customer, the entity which determines the purposes and means of the processing of Personal Data.

- **Customer Data** *means* data, which may include Personal Data and the categories of data submitted, stored, sent, or received via the Services by Customer, its Affiliates, or end users.

- **Data Protection Laws** *means* all laws and regulations applicable to the processing of Personal Data under the Agreement, including, but not limited to, the EU GDPR, the UK GDPR, the UK Data Protection Act 2018, the FDPA, the CCPA, the Privacy and the Electronic Communications Regulations 2003 (SI 2003/2426) as amended, and all other applicable data protection and privacy legislation in force from time to time (as may be applicable depending on the location of Customer, data subjects and processing of the relevant Personal Data).

- **Data Subject** *means* (i) the identified or identifiable person to whom Personal Data relates; or (ii) a "Consumer" as the term is defined in the CCPA.

- **DPA** *means* this data processing addendum and its schedules.

- **EEA** *means* the European Economic Area (namely the EU, Norway, Iceland and Lichtenstein together).

- **EU GDPR** *means* Regulation (**EU**) 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 (General Data Protection Regulation).

- **FDPA** *means* the Swiss Federal Act on Data Protection of 19 June 1992 (SR 235.1; FDPA) as amended from time to time.

- **Standard Contractual Clauses** *means* (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries and published at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN (**EU SCCs**); (ii) where the UK GDPR applies standard data protection clauses adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR (**UK SCCs**); and (iii) where Personal Data is transferred from Switzerland to outside of Switzerland or the EEA, the EU SCCs as amended in accordance with guidance from the Swiss Data Protection Authority (**Swiss SCCs**).

- **Personal Data** *means* any information relating to: (i) an identified or identifiable natural person and (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws), which is provided as Customer Data.

- **Processor** *means* SearchStax, the entity which Processes Personal Data on behalf of Controller, including as applicable any "Service Provider" as that term is defined by the CCPA.

- **Restricted Transfer** *means*: (i) where the EU GDPR applies, a transfer of Personal Data via the Services from the EEA either directly or via onward transfer, to any country or recipient outside of the EEA not subject to an adequacy determination by the European Commission; and (ii) where the UK GDPR applies, a transfer of Personal Data via the Services from the United Kingdom either directly or via onward transfer, to any country or recipient outside of the UK not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and (iii) a transfer of Personal Data via the Services from Switzerland either directly or via onward transfer, to any country or recipient outside of the EEA and/or Switzerland not subject to an adequacy determination by the European Commission.

- **Sub-processor** *means* any third party (including SearchStax Affiliates) engaged by SearchStax to process Personal Data under this DPA in the provision of the Services to Customer.

- **Supervisory Authority** *means* a governmental or government-chartered regulatory body having binding legal authority over a party.

- **Services** *means* the web subscription services provided by SearchStax to the Customer pursuant to the Agreement.

- **UK GDPR** means the EU GDPR as it forms part of the laws of the UK by virtue of section 3 of the European Union (Withdrawal) Act 2018.

1. PURPOSE.

a. SearchStax has agreed to provide the Services to Customer in accordance with the terms of the Agreement. In providing the Services, SearchStax will process Customer Data on behalf of Customer. Customer Data may include Personal Data. SearchStax will process and protect such Personal Data in accordance with the terms of this DPA and the Data Protection Laws.

b. With respect to Customer Data under this DPA, the parties agree that Customer is the 'data controller' and SearchStax is the 'data processor'. Customer will comply with its obligations as a controller and SearchStax will comply with its obligations as a processor under the DPA.

c. Where a Customer Affiliate or a Customer client is the controller with respect to certain Customer Data, Customer represents and warrants to SearchStax that it is authorized to instruct SearchStax and otherwise act on behalf of such Customer Affiliate or a Customer client in relation to Customer Data in accordance with the Agreement and this DPA.

2. SCOPE.

a. In providing the Services to Customer pursuant to the terms of the Agreement, SearchStax will treat Personal Data as confidential and only process Personal Data on behalf of Customer, and only to the extent necessary to provide Services and in accordance with the Customer's instructions as documented in the Agreement and this DPA.
b. SearchStax and Customer must take steps to ensure that any natural person acting under the authority of Customer or SearchStax who has access to Personal Data does not process the Personal Data except as specified in this DPA unless required to do so by Data Protection Laws.

3. SEARCHSTAX OBLIGATIONS.

a. SearchStax may collect, process, or use Personal Data only in accordance with the scope of the Agreement, this DPA, and Customer's instructions. This DPA is Customer's complete and final documented instruction to SearchStax in relation to Personal Data. Additional instructions outside the scope of this DPA (if any) require prior written agreement between SearchStax and Customer, including agreement on any additional fees payable by Customer to SearchStax for carrying out such instructions.
b. SearchStax will ensure that all employees, agents, officers, and contractors involved in the handling of Personal Data: (i) are aware of the confidential nature of Personal Data and are contractually bound to keep Personal Data confidential; (ii) have received appropriate training on their responsibilities as a data processor; and (iii) are bound by terms materially no less restrictive than the terms of this DPA.

c. SearchStax must maintain appropriate managerial, operational, and technical safeguards designed to preserve the integrity and security of Personal Data while in its possession and control hereunder, while taking into account the state of the art, 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.
d. SearchStax must maintain appropriate measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (i) the pseudonymisation and encryption of Personal Data; (ii) the on-going confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In accessing the appropriate level of security, SearchStax takes into account the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed, as further set forth in **Schedule 2**.
e. Customer agrees that, in the course of providing the Services to Customer, it may be necessary for SearchStax to access Personal Data to respond to any technical problems, Customer queries, security monitoring, and to ensure the proper working of the Services. All such access by SearchStax will be limited to those purposes and performed by authorized personnel.
f. SearchStax must promptly inform Customer, if in SearchStax's opinion, any of the instructions regarding the processing of Personal Data provided by Customer, breach Data Protection Laws.
g. SearchStax will reasonably assist Customer in meeting the Customer's obligation to carry out Data Protection Impact Assessments (**DPIA**), taking into account the nature of processing and the information available to SearchStax.
h. Customer and SearchStax and, where applicable, their representatives, will cooperate, upon request, with a Supervisory Authority in the performance of their respective obligations under this DPA and Data Protection Laws.
i. SearchStax may not (i) sell Personal Data; (ii) retain, use, or disclose Personal Data for commercial purposes other than providing the Services under the terms of the Agreement; or (iii) retain, use, or disclose Personal Data outside of the Agreement. SearchStax understands these restrictions.

4. CUSTOMER OBLIGATIONS.

a. Customer represents and warrants, in its use of the Services, that: (i) it will comply with the terms of the Agreement, this DPA, and the Data Protection Laws, including any applicable requirements to provide notice to and/or obtain consent from Data Subjects for Processing by SearchStax; and (ii) it will ensure that its use of the Services will not violate the rights of any Data Subjects. All Affiliates of Customer who use the Services will comply with the obligations of Customer set out in this DPA.
b. Customer represents and warrants that, as having sole responsibility for the quality, legality, and accuracy of Personal Data, has obtained any and all necessary permissions and authorizations necessary to permit SearchStax, its Affiliates, and Sub-processors, to execute their rights or perform their obligations under this DPA.
c. Customer represents and warrants that its instructions comply with Data Protection Laws.
d. Customer must inform SearchStax of any notice, inquiry (including any notice, investigation, complaint, or request) relating to SearchStax's processing of Personal Data and provide SearchStax with a copy thereof within 48 hours of receipt by Customer of such notice or inquiry. Notices should be sent to: **privacy@searchstax.com**.

5. NOTIFICATION OF SECURITY BREACH.

a. SearchStax will notify Customer without undue delay after becoming aware of (and in any event within 72 hours of discovering) any accidental or unlawful destruction, loss, alteration or unauthorized disclosure or access to Customer's Personal Data (**Personal Data Breach**).
b. SearchStax will take all commercially reasonable measures to secure Personal Data, to eliminate the Data Breach, and to assist Customer in meeting the Customer's obligations under applicable law. In the event of a Personal Data Breach, SearchStax's System Administration Team and Security Team will perform a risk-based assessment of the situation and develop appropriate strategies in accordance with SearchStax incident response procedures, which include contacting Customer's primary (technical or business) point of contact or Security Operation Center (**SOC**) to brief them on the situation and provide resolution status updates.

6. AUDIT.

a. SearchStax will make available to Customer all information reasonably necessary to demonstrate compliance with its processing obligations and allow for and contribute to audits and inspections.
b. Any audit conducted under this DPA will consist of examination of the most recent reports, certificates and/or extracts prepared by an independent auditor bound by confidentiality provisions similar to those set out in the Agreement. In the event that provision of the same is not deemed sufficient in the reasonable opinion of Customer, Customer may conduct a more extensive audit which will be: (i) at the Customer's expense; (ii) limited in scope to matters specific to Customer and agreed in advance; (iii) carried out during SearchStax's business hours and upon reasonable notice which must be not less than 4 weeks unless an identifiable material issue has arisen; and (iv) conducted in a way which does not interfere with SearchStax's day-to-day business. Any such audit must be conducted remotely, except Customer and/or its Supervisory Authority may conduct on on-site audit at SearchStax's premises if so required by the Data Protection Laws. In no event will any audit of a Sub-processor, beyond a review of reports, certifications and documentation made available by the Sub-processor, be permitted without the Sub-processor's consent. This Section does not modify or limit the rights of audit of Customer, instead it is intended to clarify the procedures in respect of any audit.

7. DATA SUBJECTS.

a. SearchStax must, to the extent legally permitted, promptly notify Customer if SearchStax receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of processing, erasure, data portability, object to the processing (**Data Subject Request**).
b. Taking into account the nature of the processing and the information available to SearchStax, SearchStax must assist Customer by having in place appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under the Data Protection Laws.
c. To the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, SearchStax must upon Customer's request, and to the extent possible, provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent SearchStax is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws. To the extent legally permitted, Customer must be responsible for any costs arising from SearchStax's provision of such assistance.

8. SUB-PROCESSORS.

a. The Customer agrees that: (i) Affiliates of SearchStax may be used as Sub-processors; and (ii) SearchStax and its Affiliates respectively may engage Sub-processors in connection with the provision of the Services. The current list of Sub-processors is in **Schedule 3**. Customer authorises SearchStax to use the Sub-processors set out in **Schedule 3**.
b. During the term of this DPA, SearchStax will provide Customer with 30 days prior notification, via email, of any changes to the list of Sub-processors before authorising any new or replacement Sub-processors to process Personal Data in connection with the provision of the Services.
c. Customer may object to the use of a new or replacement Sub-processor, by notifying SearchStax promptly in writing within 10 business days after receipt of SearchStax's notice. If Customer objects to a new or replacement Sub-processor, and that objection is not unreasonable, Customer may terminate the Agreement or applicable order with respect to those Services which cannot be provided by SearchStax without the use of the new or replacement Sub-processor. SearchStax will refund Customer any prepaid and unused fees covering the remainder of the term of the applicable order following the effective date of termination with respect to such terminated Services.
d. All Sub-processors who process Personal Data must comply with the applicable obligations of SearchStax set out in this DPA. SearchStax must prior to the relevant Sub-processor carrying out any processing activities in respect of Personal Data: (i) appoint each Sub-processor under a written contract containing materially the same obligations to those of SearchStax in this DPA enforceable by SearchStax; and (ii) ensure each such Sub-processor complies with all such obligations.
e. Customer agrees that SearchStax and its Sub-processors may make Restricted Transfers of Personal Data to countries outside of the EEA, UK, or Switzerland, for the purposes of providing the Services to Customer in accordance with the Agreement. SearchStax confirms that such Sb-processors (i) are located in a third country or territory recognized by the EU Commission or a Supervisory Authority, as applicable,

to have an adequate level of protection; or (ii) have entered into the applicable Standard Contractual Clauses with SearchStax; or (iii) have other legally recognized appropriate safeguards in place.

9. RESTRICTED TRANSFERS.

a. The parties agree that, when the transfer of Personal Data from Customer to SearchStax or from SearchStax to a Sub-processor is a Restricted Transfer, it will be subject to the applicable Standard Contractual Clauses.
b. The parties agree that the EU SCCs apply to Restricted Transfers from the EEA. The EU SCCs are deemed entered into (and incorporated into this DPA by reference) and completed as follows:
   (i) **Module Two (Controller to Processor)** applies where Customer is a Controller of Customer Data and SearchStax is processing Customer Data;
   (ii) **Module Three (Processor to Processor)** apples where SearchStax is a Processor of Customer Data and SearchStax uses a Sub-processor to process Customer Data;
   (iii) **Module Four (Processor to Controller)** does not apply;
   (iv) in **Clause 7 of the EU SSCs**, the optional docking clause will not apply;
   (v) in **Clause 9 of the EU SSCs, Option 2 applies**, and the time period for notice of Sub-processors must be as set out in Section 8.c. of this DPA;
   (vi) in **Clause 11 of the EU SSCs**, the optional language does not apply;
   (vii) in **Clause 17 of the EU SSCs, Option 1** applies, the EU SCCs are governed by Irish law, and for the Swiss SCCs, Swiss law;
   (viii) in **Clause 18(b) of the EU SSCs**, disputes must be resolved by: the courts of Ireland for the EU SCCs, and the courts of Switzerland for the Swiss SCCs;
   (ix) Annex I of the EU SCCs are deemed completed with the information set out in **Schedule 1** of this DPA; and
   (x) Annex II of the EU SCCs are deemed completed with the information set out in **Schedule 2** of this DPA.
c. The parties agree that the EU SCCs as amended in clause 9(b) above, shall be adjusted as set out below where the FDPA applies to any Restricted Transfer:
   (i) The Swiss Federal Data Protection and Information Commissioner (**FDPIC**) shall be the sole Supervisory Authority for Restricted Transfers exclusively subject to the FDPA;
   (ii) Restricted Transfers subject to both the FDPA and the EU GDPR, shall be dealt with by the EU Supervisory Authority named in **Schedule 1** of this DPA;
   (iii) The term 'member state' must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU SCCs;
   (iv) Where Restricted Transfers are exclusively subject to the FDPA, all references to the GDPR in the EU SCCs are to be understood to be references to the FDPA;
   (v) Where Restricted Transfers are subject to both the FDPA and the EU GDPR, all references to the GDPR in the EU SCCs are to be understood to be references to the FDPA insofar as the Restricted Transfers are subject to the FDPA; and
   (vi) The Swiss SCCs also protect the Personal Data of legal entities until the entry into force of the revised FDPA.
d. The parties agree that the UK SCCs apply to Restricted Transfers from the UK and the UK SCCs are deemed entered into (and incorporated into this DPA by reference), completed as follows: (i) Appendix 1 of the UK SCCs are deemed completed with the information set out in **Schedule 1** of this DPA; and (ii) Appendix 2 of the UK SCCs are deemed completed with the information set out in **Schedule 2** of this DPA.
e. If any provision of this DPA contradicts any Standard Contractual Clauses, the provisions of the applicable Standard Contractual Clauses prevail over this DPA.

10. LIABILITY.

a. The parties agree that SearchStax is liable for any breaches of this DPA caused by the acts and omissions of its Sub-processors to the same extent SearchStax would be liable if performing the services of each Sub-processor directly under the terms of this DPA.
b. The parties agree that Customer is liable for any breaches of this DPA caused by the acts and omissions of its Affiliates and users as if such acts and omissions had been committed by Customer itself.
c. **The limitations of liability in the Agreement apply to all claims related to or arising under this DPA.**

11. TERM AND TERMINATION.

SearchStax will only process Personal Data for the term of this DPA. The term of this DPA coincides with the beginning of the Agreement and this DPA will automatically terminate upon the termination of the Agreement.

12. DELETION AND RETURN OF PERSONAL DATA.

a. SearchStax will, upon written request and at the choice of Customer, either: (i) make the Services available to Customer for the return Personal Data to Customer at the expiration of the order within the time periods set out in termination section of the Agreement, or (ii) securely delete all Personal Data. SearchStax will securely delete all Personal Data after such time period, unless law applicable to SearchStax prevents destruction of Personal Data; and upon request, provide a certification of deletion of Personal Data.
b. Where any Personal Data is retained beyond termination of this DPA, Personal Data must be treated as Confidential Information and will no longer be actively processed.

13. GENERAL.

a. This DPA sets out the entire understanding of the parties, and supersedes all prior and contemporaneous agreements and understandings, with regards to the subject matter. No modification or waiver of any term in this DPA is effective unless both parties sign it.
b. Should a provision of this DPA be invalid or become invalid, then the legal effect of the other provisions will be unaffected. A valid provision is deemed to have been agreed upon, which comes closest to what the parties intended commercially and will replace the invalid provision. The same will apply to any omissions.
c. To the extent of any conflict or inconsistency, the following order of precedent applies: the applicable Standard Contractual Clauses, followed by the Agreement, and then this DPA, *provided that,* in all instances the disclaimer of damages and limitation of liability in the Agreement applies. Subject to the amendments in this DPA, the Agreement remains in full force and effect.
d. Customer may send any questions or concerns regarding this DPA to: privacy@searchstax.com.

_____(Customer)	**SearchStax, Inc.**
Signature:	Signature:
Printed Name:	Printed Name:
Title:	Title:
Date:	Date:
Address:	Address: 101 Continental Blvd, Suite 210 El Segundo, CA 90245 USA

Schedules Attached:

Schedule 1 - List of Parties and Categories of Data
Schedule 2 - Technical and Organizational Security Measures
Schedule 3 - List of Sub-Processors

SCHEDULE 1

List of Parties, Description of Processing and Transfer of Personal Data, Competent Supervisory Authority

MODULE TWO: CONTROLLER TO PROCESSOR

A. LIST OF PARTIES

The Controller:

Controller Entity:	Customer
Address:	As set out for Customer in the Agreement.
Contact person's name, position and contact details:	As provided by Customer in its account and used for notification and invoicing purposes.
Activities relevant to the data transferred under the SCCs:	Use of the Services.
Signature and date:	By entering into the Agreement, the Controller is deemed to have signed the SCCs incorporated into this DPA and including their Annexes.
Role:	Data Exporter.
Name of Representative (if applicable):	Any UK or EU representative named in the Controller's privacy policy.

The Processor:

Processor Entity:	SearchStax
Address:	As set out for SearchStax in the Agreement.
Contact person's name, position and contact details:	As provided by SearchStax in its account and used for notification and invoicing purposes.
Activities relevant to the data transferred under the SCCs:	The provision of cloud computing solutions to the Controller under which the Processor processes Personal Data upon the instructions of the Controller in accordance with the terms of the Agreement.
Signature and date:	By entering into the Agreement, the Processor is deemed to have signed the SCCs, incorporated into this DPA, including their Annexes.
Role:	Data Importer.

B. DESCRIPTION OF PROCESSING AND TRANSFERS

Categories of data subjects:	Customers of the Controller.
Categories of personal data:	The Controller may submit personal data to the Services, the extent of which is determined and controlled by the Controller. The personal data includes but is not limited to: 1. First, Middle and Last Name (current and former) 2. Title 3. Position 4. Employer 5. Personal and Business Contact Information (company, email, physical address, phone number) 6. ID data 7. Professional life data 8. Personal life data 9. Connection data 10. Localization data
Sensitive Data:	No sensitive data will be processed or transferred and may not be contained in the content of or attachments to emails.
The frequency of the processing and transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous basis for the duration of the Agreement.
Nature of the processing:	SearchStax processes Personal Data to the extent necessary to perform the Services under the Agreement, as further instructed by Customer pursuant to this DPA.
Purpose(s) of the data transfer and further processing:	Personal Data is transferred to sub-contractors who need to process some of Personal Data in order to provide their services to the Processor as part of the Services provided by the Processor to the Controller.
The period for which Personal Data will be retained, or, if that is not possible, the criteria used to determine that period:	Unless agreed otherwise in writing, for the duration of the Agreement, subject to Section 11 of this DPA.
For transfers to (Sub-) processors, also specify subject matter, nature and duration of the processing:	The Sub-processor list set forth in Schedule 3 sets out Personal Data processed by each Sub-processor and the services provided by each Sub-processor.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies (e.g. in accordance with Clause 13 of the SCCs)	Where the EU GDPR applies, the Data Protection Authority in Ireland. Where the UK GDPR applies, the UK Information Commissioner's Office (ICO). Where the FDPA applies, the Swiss Federal Data Protection and Information Commissioner (FDPIC).

MODULE THREE: PROCESSOR TO PROCESSOR

A. LIST OF PARTIES

The Data Exporter: is SearchStax.

The Data Importers: are the Sub-processors named in the Sub-processor list which contains the name, address, contact details and activities relevant to the data transferred to each Data Importer.

B. DESCRIPTION OF PROCESSING AND TRANSFERS

The Sub-processor list includes the information about the processing and transfers of Personal Data, for each Data Importer:

- categories of data subject;
- categories of Personal Data;
- the nature of the processing; and
- the purposes of the processing.

Personal Data is processed by each Sub-processor:

- on a continuous basis;
- to the extent necessary to provide the Services in accordance with the Agreement and the Data Exporter's instructions; and
- for the duration of the Agreement and subject to Section 11 of this DPA.

C. COMPETENT SUPERVISORY AUTHORITY

The competent Supervisory Authority of each Sub-processor are listed below:

- Where the EU GDPR applies, the Member State in which the Sub-processor has its EU representative;
- Where the UK GDPR applies, the UK Information Commissioner's Office (ICO); and
- Where the FDPA applies, the Swiss Federal Data Protection and Information Commissioner (FDPIC).

SCHEDULE 2

TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

(Including Technical and Organizational Measures to Ensure the Security of Data)

Below is a description of the technical and organizational measures implemented by the Processor(s) / Data Importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Where applicable this Schedule 2 will serve as Annex II to the SCCs.

Measure	Description
Measures for screening employees prior to employment	*The processor conducts background checks of all employees. Employment offer is contingent upon a successful background check*
Measures for training employees on information security risks	*The processor has implemented formal processes for training its employees on security best practices, and for evaluating their understanding of the concepts*
Measures for clearly defining roles and responsibilities for information security and privacy	*The processor has defined roles for security and privacy governance and operations*
Measures for assessment of risks pertinent to the environment	*The processor has implemented formal information security risk management processes, which include identification of inherent risks, control effectiveness and residual risks in the environment*
Measures for secure development and implementation of software and systems	*The processor has implemented secure software development procedures which include secure design, secure coding and vulnerability testing.*
Measures for protection of source code	*The processor has implemented strong access controls for source code repositories, which include logging of security events.*
Measures for encryption of personal data	*The processor's archived data is encrypted at rest using AES256 bit encryption and data in transit is protected by Transport Layer Security ("TLS").*
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	*Access to data necessary for the performance of the particular task is ensured within the systems and applications by a corresponding role and authorization concept. In accordance with the "least privilege" and "need-to-know" principles, each role has only those rights which are necessary for the fulfilment of the task to be performed by the individual person.* *To maintain data access control, state of the art encryption technology is applied to Personal Data itself where deemed appropriate to protect sensitive data based on risk.*
Measures for ensuring the ability to restore the availability and access to personal data in a timely	*The processor has implemented disaster recovery processes, which include provisioning of a secondary disaster recovery region, and development of procedures to facilitate a failover in the event of a disaster.*

Measure	Description
manner in the event of a physical or technical incident	
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	*The processor performs monthly testing to identify vulnerabilities in its networks and applications. Additionally, the processor performs an independent penetration test on an annual basis.*
Measures for user identification and authorization	*Remote access to the data processing systems is only possible through use of processor's provisioned identity and jump servers. All access attempts, successful and unsuccessful are logged and monitored.*
Measures for ensuring physical security of locations at which personal data are processed	*The processor uses a sub-processor whose facilities are used to host systems containing personal data. The facilities are protected by industry leading physical security standards including badge access systems and 24x7 CCTV monitoring*
Measures for ensuring events logging	*System inputs are recorded in the form of log files therefore it is possible to review retroactively whether and by whom personal data was entered, altered or deleted.*
Measures for monitoring of security events	*Processor has implemented systems that can be used for monitoring security events in the data processing environment, as well as procedural measures to monitor the output from security event monitoring systems.*
Measures for responding to security events	*Processor has implemented procedures to respond to security events that are identified. Response procedures include mitigating cyber threats, remediation, as well as, if required, notification of customers, regulators and law enforcement agencies.*
Measures for internal IT and IT security governance and management	*Example: Employees are instructed to collect, process and use personal data only within the framework and for the purposes of their duties (e.g. service provision). At a technical level, multi-client capability includes separation of functions as well as appropriate separation of testing and production systems.* *The Controller's personal data is stored in a way that logically separates it from other customer data.*
Measures for certification/assurance of processes and products	*The Processor utilizes third party data centers that maintain current SOC 2 Attestation Reports. The Processor will not utilize third party data centers that do not maintain the aforementioned certifications and/or attestations, or other substantially similar or equivalent certifications and/or attestations.* *Additionally, the processor maintains current SOC 2 attestation report for the data processing environment.* *Upon the Controller's written request (no more than once in any 12 month period), the Processor must provide within a reasonable time, a copy of the most recently completed certification and/or attestation reports (to the extent that to do so does not prejudice the overall security of the Services). Any audit report submitted to the Controller must be treated as Confidential Information and subject to the confidentiality provisions of the Agreement between the parties.*

SCHEDULE 3

LIST OF SUB-PROCESSORS

INFRASTRUCTURE:

We use the following sub-processors to provide our cloud infrastructure environment and storage of our Customer Content:

SUBPROCESSOR	CORPORATE LOCATION
Amazon Web Services, Inc.	USA
Microsoft Corporation	USA
Google, Inc.	USA

PROCESSING OF CUSTOMER CONTENT:

We work with various sub-processors that monitor, maintain and otherwise support the Services. In order to provide this functionality these sub-processors may, but not necessarily will, have access to Customer Content:

COMPANY NAME	CORPORATE LOCATION	PURPOSE
Paypal, Inc.	USA	Credit Card Processing
Zendesk, Inc.	USA	Customer Account Administration and Support
Google, Inc.	USA	Email, Calendar, Office Products
Salesforce.com, Inc.	USA	Sales and Account Management
HubSpot, Inc.	USA	Marketing Automation
The Rocket Science Group, LLC d/b/a MailChimp	USA	Email Marketing
Xero Limited	USA	Accounting
Atlassian Pty Ltd.	USA	Bug Tracking
PagerDuty Inc.	USA	Service Monitoring and Alerting
Datadog, Inc.	USA	Service Monitoring and Alerting

COMPANY NAME	CORPORATE LOCATION	PURPOSE
Slack, Inc.	USA	Customer Support Tool
Dropbox, Inc.	USA	Document Storage
Mixpanel, Inc.	USA	Customer Account Administration and Support
ChurnZero, Inc	USA	Customer Success Tool
Monday.com	USA	Collaboration Tool

SEARCHSTAX GROUP SUB-PROCESSORS:

COMPANY NAME	LOCATION
SearchStax, Inc.	USA
SearchStax India Pvt. Ltd.	India