Data Processing Addendum

This Data Processing Addendum, together with all applicable appendices and annexes ("DPA"), is effective upon execution of an order form and/or the underlying Agreement by and between Sawtooth Software, Inc., a Utah corporation ("Sawtooth") and the party named as Customer in the order form and/or underlying Agreement. This DPA reflects the parties' agreement with regards to the applicable Data Protection Laws and Regulations. Customer acknowledges that this DPA constitutes a binding and enforceable legal contract between Customer and Sawtooth. This Agreement requires execution by authorized representative from each party.

How This DPA Applies

The terms of this DPA only apply to Customer and Sawtooth as follows:

A. When Customer subscribes to Sawtooth's web hosting and/or requires Sawtooth to Process/transfer Customer's Data Subjects Data collected in the European Union (EU) or European Economic Areas (EEA), Sections 1 through 8 and Appendix 1-A and Appendix 1-B shall apply to the underlying Agreement.

B. When Customer subscribes to Sawtooth's web hosting and/or requires Sawtooth to Process/transfer Customer's Data Subjects Data collected in the United Kingdom (UK), Sections 1 through 8, Appendix 1-B, and Appendix 2 apply to the underlying agreement.

C. When Customer subscribes to Sawtooth's web hosting and/or requires Sawtooth to Process/transfer Customer's Data Subjects Data collected in the United States (US), then only applicable Sections 1 through 8 apply to the parties.

D. When Customer subscribes to Sawtooth's web hosting and/or requires Sawtooth to Process/transfer Customer's Data Subjects Data collected in the EU, UK, and US, the entire DPA along with all appendices apply to the underlying Agreement.

1. Definitions

Any capitalized terms not defined herein shall have the meaning given to that term in the Agreement or applicable Data Protection Laws and Regulations.

"Data Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"Data Processor" means the entity which Processes Personal Data on behalf of the Data Controller.

"Data Protection Laws and Regulations" means the laws and regulations, including EU General Data Protection Regulation ("GDPR"), country specific laws and regulations of the EU member states, UK Data Protection and Digital Information Bill ("DPDI"), and state specific privacy acts in the United States may be applicable to the Processing of Personal Data with the Service under the Agreement.

"Data Protection Supervisory Authority/ies" means a supervisory authority or other government body responsible for the administration, implementation, and/or enforcement of Data Protection Laws and Regulations and includes without limitation, competent supervisory authorities of the EU and its member

states, the Swiss Federal Data Protection and Information Commissioner, and the UK Information Commissioner's Office.

"Data Subject" means the individual to whom Personal Data relates.

"Personal Data" means any information (i) of an identified or identifiable person and (ii) of an identified or identifiable legal entity (where protected under applicable Data Protection Laws and Regulations), where such data is submitted to the Service.

"Process" or "Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

"Sawtooth" means Sawtooth Software, Inc. and its affiliates and subsidiaries.

"Service" means as defined in the Agreement and set forth in the Order Form, the web hosting subscription along, or the subscription package of software/Application as a service provided by Sawtooth.

"Standard Contractual Clauses" means, when applicable, for the transfers of Personal Data out of the EEA and Switzerland, the agreement executed by and between Customer and Sawtooth and attached hereto as Appendix 1-A pursuant to the European Commission's decision of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council, and for the transfers of Personal Data out of the UK, the agreement executed by and between Customer and Sawtooth and attached hereto as Appendix 2 in accordance with the UK Data Protection Act 2018 on 2 February 2022 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

"Sub-processor" means any third party appointed by or on behalf of Sawtooth to Process Personal Data in connection with the Service.

2. Processing of Personal Data

a. Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Data Controller and Sawtooth is a Data Processor.

b. Customer's Responsibilities. Customer shall, in Customer's use of the Service, submit or make available Personal Data to Sawtooth for Processing in accordance with the requirements of Data Protection Laws and Regulations, and Customer's instructions to Sawtooth for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the initial accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

c. Customer's Instructions. Sawtooth shall only Process Personal Data on behalf of and in accordance with Data Protection Laws and Regulations in EU, UK, and California in the US, Customer's instructions (including as is necessary to provide the Service to Customer under the Agreement). Customer instructs Sawtooth to Process Personal Data for the following purposes: (i) for the performance of the Agreement and applicable Order Form(s), including to provide Service to the Customer and to communicate with Customer; (ii) to store survey data collected by Customer for the duration of the Service plus ninety (90) days in the backup system; (iii) to archive business transaction related communications in order to refresh memory and in case of

any dispute or controversy; and (iv) for any other purposes reasonably instructed by Customer in writing (e.g., via email *or amendment of the Agreement*).

3. Rights of Data Subjects

a. Correction, Blocking, and Deletion. To the extent that Customer, in Customer's use of the Service, does not have the ability to correct, amend, block, or delete Personal Data, as required by Data Protection Laws and Regulations, Sawtooth shall reasonably assist Customer in facilitating such actions to the extent Sawtooth is legally permitted to do so.

b. Data Subject Requests. Sawtooth shall, to the extent legally permitted, promptly notify Customer if Sawtooth receives a request from a Data Subject for access to, correction, amendment, or deletion of that Data Subject's Personal Data. If legally permitted, Sawtooth shall not respond to any such Data Subject request without Customer's prior written consent except to confirm that the request relates to Customer. In the case of a legal demand for disclosure of Personal Data in the form of a subpoena, search warrant, court order, or other compulsory disclosure request, Sawtooth shall attempt to redirect the requesting party or agency to request disclosure from Customer. Customer agrees that Sawtooth may provide Customer's basic contact information for this purpose. Sawtooth shall reasonably cooperate and assist in relation to the handling of a Data Subject's request for access to that person's Personal Data, to the extent legally permitted and to the extent Sawtooth only has limited access to such Personal Data through provide of the Service.

4. Sawtooth Personnel

a. Confidentiality. Sawtooth shall take reasonable actions to ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities, and have executed written confidentiality agreements. Sawtooth shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

b. Limitation of Access. Sawtooth shall take reasonable actions to ensure that Sawtooth's access to Personal Data is limited to those personnel who require such access to perform under the Agreement.

5. Security

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, Sawtooth shall implement reasonable technical and organizational measures designed to ensure a level of security appropriate to the risk and as detailed in Annex 2. Sawtooth regularly monitors compliance with these safeguards. Sawtooth may update these technical and organization measures from time to time, but Sawtooth will not materially decrease the overall security of the Service.

6. Security Breach Management and Notification

Sawtooth maintains security incident management policies and procedures and shall, to the extent permitted by law, without undue delay, and in any event within 72 hours of becoming aware, notify Customer of any actual or reasonably suspected unauthorized access, use, modification, or disclosure of Personal Data (a "Security Breach"). The notice shall summarize in reasonable detail the nature and scope of the Security Breach, to the extent known, and the corrective action already taken or to be taken by Sawtooth. Furthermore, Sawtooth shall provide timely information relating to the Security Breach as it becomes known or as reasonably requested by Customer. Sawtooth shall make reasonable efforts to identify and promptly take all reasonable steps to remediate the cause of such Security Breach. Sawtooth shall not publicly disclose any information regarding the Security Breach without Customer's

prior written consent, except (i) to its own employees, customers, advisors, agents, or contractors or (ii) where and to the extent explicitly compelled to do so by Data Protection Laws and Regulations, to Data Protection Supervisory Authorities and/or Data Subjects. Unless prohibited by an applicable statute or court order, Sawtooth shall also notify Customer of any third-party legal process relating to any Security Breach, including but not limited to, any legal process initiated by any governmental entity. Customer's contact person and info in the event of a Security Breach:

7. Government Interception/Inspection

In the event that Sawtooth is notified that any part of the Processing under this Agreement will be the subject of an interception or inspection by any duly authorized agency of the federal, state, local or any foreign government, or in the event that Sawtooth is not so notified, but at some point in the conduct of such an interception or inspection, any part of the Processing appears to be involved, Sawtooth agrees to follow the procedures set forth below: Unless prohibited by law or the government, Sawtooth shall promptly advise the Customer contact set forth in Section 6 by email with an explanation of the circumstances of any such inspection and, if possible, which part of the Processing provided by Sawtooth for Customer is or might become involved. Unless otherwise required by law, Sawtooth agrees not to permit any inspections involving the Processing of data provided by Customer to Sawtooth nor to disclose any related Customer Data until further instructions are received from Customer.

8. Additional Terms

a. Application of Standard Contractual Clauses. The Standard Contractual Clauses in Appendix 1-A and the additional terms in Section 7 will apply to the Processing of Personal Data by Sawtooth in the course of providing Services as follows:

    i. Notwithstanding anything to the contrary in this DPA, the Standard Contractual Clauses apply only to Personal Data that is transferred from the EEA and/or Switzerland and the UK to outside the EEA and Switzerland or the UK, either directly or via onward transfer, to any country or recipient not recognized by the European Commission or other Data Protection Supervisory Authority (as applicable) as providing an adequate level of protection for personal data (as described in the EU Data Protection Directive or its successors).

    ii. Subject to Section 7.a(i), the Standard Contractual Clauses apply to (i) the legal entity that has executed the Agreement and is the Controller and, (ii) all Affiliates (as defined in the Agreement) of Customer established within the EEA and Switzerland or the UK that have licensed the Service. For the purpose of the Standard Contractual Clauses and this Section 7, the aforementioned entities shall be deemed "Controllers".

b. Objective and Duration. The objective of Processing of Personal Data by Sawtooth is the provision of the Service pursuant to the Agreement for the term(s) of the Agreement.

c. Sub-processors. Pursuant to this DPA and the Standard Contractual Clauses, Customer acknowledges and expressly agrees that: (a) Sawtooth's Affiliates may be retained as Sub-processors; and (b) Sawtooth and Sawtooth's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Service or support services.

    i. Liability. Sawtooth shall be liable for the acts and omissions of its Sub-processors to the same extent Sawtooth would be liable if performing the services of each Sub-processor directly.

    ii. List of Current Sub-processors and Notification of New Sub-processors. A list of current Sub-processors for the Service is available upon request and Customer agrees to Sawtooth's use of the listed Sub-processors as of the execution of this DPA. Sawtooth shall notify Customer if it adds or replaces any Sub-processors prior to any such changes

if Customer subscribes to such notifications by sending an email to privacy@sawtoothsoftware.com with the subject line “Sub-processor Notification Request” (or by other means established by Sawtooth and communicated to Customer from time to time) This notification process is Sawtooth’s only responsibility for notifying Customer of a new Sub-processor.

iii. Objection to Sub-processors. Customer may object in writing to Sawtooth’s appointment of a new Sub-processor on reasonable grounds relating to data protection (e.g., if making Personal Data available to the Sub-processor may violate applicable Data Protection Laws) by notifying Sawtooth promptly in writing within fifteen (15) calendar days of receipt of Sawtooth’s notice in accordance with Section 7.3.2 above. Such notice shall explain the reasonable grounds for the objection and the parties shall discuss such concerns in good faith with a view to achieving commercially reasonable resolution. If no such resolution can be reached, Sawtooth will, at its sole discretion, either not appoint that proposed Sub-processor, or permit Customer in writing to suspend or terminate the affected Service in accordance with the termination provisions in the Agreement without liability to either party (but without prejudice to any fees incurred by Customer prior to suspension or termination).

iv. Sub-processor Agreements. Sawtooth or a Sawtooth Affiliate has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this Agreement to the extent applicable to the nature of the services provided by such Sub-processor.

d. Audits and Certifications. The parties agree that the audits described in the Standard Contractual Clauses and otherwise required by Applicable Data Protection Laws and Regulations shall be carried out in accordance with the following specifications:

i. Upon Customer’s request, and subject to the confidentiality obligations set forth in the Agreement, Sawtooth shall make available to Customer (or Customer’s independent, third-party auditor that is not a competitor of Sawtooth) information demonstrating Sawtooth’s compliance with the obligations set forth in this DPA in the form of the certifications and audit reports for the Services. In the event Customer does not find the certifications and audit reports suitable, Sawtooth will make its applicable premises and personnel available to Customer for audit upon request but no more than once annually and at Customer’s expense. Before the commencement of any such audit, Customer and Sawtooth shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources provided by Sawtooth. Customer shall promptly notify Sawtooth with information regarding any non-compliance discovered during the course of an audit and all findings during the audit shall be considered confidential information between Customer and Sawtooth except as expressly required otherwise by Data Protection Laws and Regulations.

e. Return and Deletion of Personal Data. Where applicable based on the Service, Sawtooth will return and delete Personal Data in accordance with the Agreement. Customer is responsible for the correction, amendment, blocking, or deleting of Personal Data within its control within the Service.

f. Impact Assessments and Prior Consultation. To the extent Sawtooth is required under Data Protection Laws and Regulations, Sawtooth will provide reasonably requested information regarding Sawtooth’s processing of Customer Data under the Agreement, to the extent Customer does not otherwise have access to confidential or a third-party information outside the scope of work and to the extent that such information is available to Sawtooth, to enable the Customer to carry out data protection/transfer impact assessments or prior consultations with supervisory authorities as required by law.

9. General Provisions.

a. Liability for data processing. Each party's aggregate liability for any and all claims whether in contract, tort (including negligence), breach of statutory duty, or otherwise arising out of or in connection with this DPA, unless prohibited under applicable laws, shall be subject to Section 10 (LIMITATION OF LIABILITY FOR ALL CLAIMS AND DISPUTES) in the applicable custom/online subscription agreement or the Limitation of Liability section of the Terms of Use.

b. Conflict. In the case of conflict or ambiguity between: (i) the terms of this DPA and the terms of the applicable custom/online subscription agreement or the Terms of Use, with respect to the subject matter of this DPA, the terms of this DPA shall prevail; (ii) the terms of any provision contained in this DPA and any provision contained in the Standard Contractual Clauses, the provision in the Standard Contractual Clauses shall prevail.

c. Independent Processing. Customer remains exclusively liable for its own compliance with Data Protection Legislation with respect to any independent collection and processing of personal data unrelated to the Services. Customer will provide its own clear and conspicuous privacy notices that accurately describe how it does this, and Sawtooth will not be liable for any treatment of personal data by Customer in those circumstances. Customer hereby indemnifies Sawtooth in full for any and all claims or liability arising as a result of such collection and use of personal data by it in those circumstances.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed by the duly authorized representative of each party as of the signing date. This Agreement is not valid until both parties confirm the receipt of a fully executive Agreement.

Company Name: _____	Sawtooth Software Inc.
Signature: _____	**Signature:** _____
Printed Name: _____	**Printed Name:** _____Gary Baker_____
Title at Company: _____	**Title at Company:** _____COO_____
Date: _____	**Date:** _____

APPENDIX 1-A

ANNEX

Standard Contractual Clauses

Section I

Clause 1

Purpose and Scope

- The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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) for the transfer of data to a third country.

- The Parties:

    1. the natural or legal person(s), public authority/ies, agency /ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I (hereinafter each 'data exporter'), and

    2. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I (hereinafter each 'data importer')

  have agreed to these standard contractual clauses (hereinafter: 'Clauses').

- These Clauses apply with respect to the transfer of personal data as specified in Annex I.

- The Appendix 1-A to these Clauses containing the Annexes in Appendix 1-B referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

- These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix 1-A. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

- These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

- Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions;

    - Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
    - Clause 8.1(b), 8.9(a), (c), (d) and (e);
    - Clause 9(a), (c), (d) and (e);
    - Clause 12(a), (d) and (f);
    - Clause 13;
    - Clause 15.1(c), (d), and (e);
    - Clause 16(e);
    - Clause 18(a) and (b).

- Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

- Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

- These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

- These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred are specified in Annex I.

Clause 7

Docking clause

[Intentionally Omitted]

Section II – Obligations of the Parties

Clause 8

Data Protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

- The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

- The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix 1-B as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix 1-B to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

- The data importer and, during transmission, also the data exporter shall implement appropriate technical and organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration,

unauthorized disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymization, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organizational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

- The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

- In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter 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.

- The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:
(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

- The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

- The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

- The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

- The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

- The data importer has the data exporter's general authorizations for the engagement of sub-processor(s) from an agreed list, which as of the date of the Agreement, is set forth in Annex III. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least ten (10) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
- Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

- The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

- The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall

notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

- The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

- The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorized to do so by the data exporter.

- The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organizational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

- In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

- The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

- In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

- Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

    - lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

    - refer the dispute to the competent courts within the meaning of Clause 18.

- The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

- The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

- The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

- Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

- The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

- Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

- The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

- Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

- The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

- The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

[Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, as indicated in Annex I, shall act as competent supervisory authority.

The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

Section III – Local laws and practices affecting compliance with the Clauses

Clause 14

Local laws and practices affecting compliance with the Clauses

- The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorizing access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

- The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

    - the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved, and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

    - the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

    - any relevant contractual, technical, or organizational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

- The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

- The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

- The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

- Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfill its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

- The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary, with the help of the data exporter) if it:
    - receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
    - becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimization

- The data importer agrees to review the legality of the request for disclosure, in particular, whether it remains within the powers granted to the requesting public authority, and to challenge the

request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

- The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

- The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

Section IV – Final Provisions

Clause 16

Non-compliance with the Clauses and termination

- The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

- In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

- The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

    - the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

    - the data importer is in substantial or persistent breach of these Clauses; or

    - the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data

importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

- Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Cyprus.

Clause 18

Choice of forum and jurisdiction

- Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- The Parties agree that those shall be the courts of Cyprus.
- A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX 1-B

ANNEX I

A. LIST OF PARTIES - MODULE TWO (i.e., transfer controller to Processor) AND MODULE FOUR (i.e., transfer processor to controller).

Data Exporters Information

a. Data exporter: Customer

Data Protection Officer:
Address:
Contact:
Position:
Email:
Activities relevant to the data transferred under these Clauses:
Collecting, controlling, managing, and transferring survey data (basic personal identifiable information if any) via Software and web hosting.
Signature and date:
Role (controller/Processor): Controller (for the Survey Respondents Data).

b. Data exporter (not a joint controller with Customer and only applicable if Customer provides Customer Data to Sawtooth Software UK Ltd. prior to onward transfer to Sawtooth Software Inc.): Sawtooth Software UK Ltd.

Data Protection Officer: DPO
Address: C/O Monetta Llp, 232 Stamford Street Central, Ashton-Under-Lyne, United Kingdom, OL6 7NQ
Contact: DPO
Position: DPO
Email: dpo@sawtoothsoftware.com
Activities relevant to the data transferred under these Clauses:
Collecting, controlling, managing, and transferring Customer or perspective Customer information and personal data from the UK office to the US office.
Signature and date:
Role (controller/Processor): Processor (for the Customers data).

Data Importers Information.

a. Data importer: Sawtooth Software, Inc.

Data Protection Officer: DPO
Address: 3210 N. Canyon Rd., Suite 202, Provo, Utah, 84604, USA
Contact: DPO
Position: Data Protection Officer
Email: dpo@sawtoothsoftware.com
Activities relevant to the data transferred under these Clauses:
Transmitting, transferring, storing, and analyzing the collected survey data from Data Subject's premises to the default Data Center in Dallas, Texas, USA and/or from whichever Data Center location that the Customer decides to User's premises for further data Processing and data analysis.
Signature and date:
Role (controller/Processor): Processor.

b. Data importer(s):

1. Rackspace Technology

Data Protection Officer: Joanne Flack
Address: 1 Fanatical Pl, Windcrest, TX 78218, USA
Contact person: Account Executive
Position: Account Executive
Email: privacy@rackspace.com
Activities relevant to the data transferred under these Clauses:
Conducting/facilitating cloud storage and cloud migration.
Signature and date: Unable to obtain.
Role (controller/Processor): Sub-processor.

2. Amazon Web Services, Inc.

Address: 410 Terry Avenue North Seattle, WA 98109 United States
Contact: AWS Compliance Reports Support - Amazon Web Services
Position: Data Protection Officer
Activities relevant to the data transferred under these Clauses:
Conducting/facilitating cloud storage and cloud migration.
Signature and date: Unable to obtain.
Role (controller/Processor): Sub-processor.

3. Microsoft Azure

Address: One Microsoft Way, Redmond, Washington, U.S.A.
Contact: Microsoft-Report a Privacy Concern
Position: Data Protection Officer
Activities relevant to the data transferred under these Clauses:
Conducting/facilitating cloud storage and cloud migration.
Signature and date: Unable to obtain.
Role (controller/Processor): Sub-processor.

4. Stova

Address: 13 Marshall Street, Suite One, Norwalk, CT 06854
Contact: Data Protection Officer
Position: Data Protection Officer
Email: privacy@stova.io.
Activities relevant to the data transferred under these Clauses:
Processing event registrant information.
Signature and date: Unable to obtain.
Role (controller/Processor): Sub-processor.

5. Salesforce Inc.

Address: 415 Mission Street, 3rd Floor, San Francisco, CA 94105
Contact: Data Protection Officer
Position: Data Protection officer
Email: privacy@salesforce.com
Activities relevant to the data transferred under these Clauses:
Processing prospective customers and existing customers' contact information and sales related documents and notes.
Signature and date: Unable to obtain.
Role (controller/Processor): Sub-processor.

6. Oracle NetSuite

Address: 2300 Oracle Way, Austin, TX 78741
Contact: Data Protection Officer
Position: Data Protection Officer
Email: Infonetsuite_WW@oracle.com
Activities relevant to the data transferred under these Clauses:
Processing invoices, managing help support, and processing accounts receivable and payable contact information.
Signature and date: Unable to obtain.
Role (controller/Processor): Sub-processor.

7. DocuSign

Address: 221 Main St., Suite 1550, San Francisco, CA 94105
Contact: Data Protection Officer
Position: Data Protection Officer
Email: privacy@docusign.com
Activities relevant to the data transferred under these Clauses:
Generating contract execution process and storing signatures, timestamps, and signatories and stakeholders' personal information.
Signature and date: Unable to obtain.
Role (controller/Processor): Sub-processor.

8. Bettermode

Address: 22 Wellesley St E, Toronto, Ontario, Canada
Contact: Data Protection Officer
Position: Data Protection Officer
Email: dpo@bettermode.com
Activities relevant to the data transferred under these Clauses:
Providing a customizable community forum for Sawtooth account users/forum members.
Signature and date: Unable to obtain.
Role (controller/Processor): Sub-processor.

B. DESCRIPTION OF TRANSFER FOR MODULE TWO (i.e., transfer controller to Processor) AND MODULE FOUR (i.e., transfer processor to controller).

Categories of Data Subjects whose personal data is transferred:

1. Customer shall list all foreseeable categories of Data Subjects here (please ask your survey design team. For examples: children, customers, perspective customers, employees, multiple, patients, students, subscribers, users, and vulnerable adults. Please list all that apply.)

2. No child under the age of 16 is permitted unless his or her legal guardian provides written consent after reading GDPR, CCPA, or other applicable laws and regulations required notices.

Note to Customer: Whether the survey data includes any Data Subjects that require special care under the applicable laws and regulations would be determined by the Customer, and Sawtooth relies on the Customer to disclose the types/categories of Data Subjects that Customer intends to survey and request for their information as soon as that information is known to Customer, or Customer should have known, and continue to update Sawtooth in order to assess the appropriate security measures.

Categories of personal data transferred:

1. Customer shall list all foreseeable categories of personal data here (please ask your survey design

team. For examples: basic personal identifiers, criminal convictions/offenses, data revealing racial/ethnic origin, economic and financial data, gender reassignment data, genetic or biometric data, health data, identification data, location data, multiple, official documents, political opinions, religious or philosophical beliefs, sex life data, sexual orientation data, and trade union membership.)

Note to Customer: Sawtooth permits limited Personal Data, such as survey respondents' IP address, identifier number, and other non-sensitive information (i.e., information that is not categorized as sensitive information in accordance with GDPR, CCPA, or other applicable laws and regulations) if necessary to be collected from and submitted by the survey respondents and to be transferred from Customer to Sawtooth for processing. Majority of the data to be collected should be Survey Respondents' elected choices to be turned into statistical data for analysis, not for the purposes of re-identifying the survey respondents, creating, storing, or managing the personal profile of each survey respondent, or processing and transferring detailed Personal Data from any Data Subject.

Sensitive data or special data categories transferred:
Controller shall not input or collect any sensitive data (i.e., any information listed as sensitive information/data under GDPR, CCPA, or other applicable laws and regulations) or any data covered under HIPAA via any of the Sawtooth's software or online application. Sawtooth's software and online applications are not intended to be used to collect/Process or transfer sensitive data or HIPAA data. Controller shall not email, transmit, or disclose any sensitive data or HIPAA data to Sawtooth, Sawtooth's Affiliates, or Sawtooth's employees and agents.

Nature of the Processing:
Sawtooth intends to webhost survey data collected by the Controller and the Conjoint and/or MaxDiff analysis derived from the survey data. The actual survey data processed is wholly controlled by the Controller.

Description of the Processing:
In general, Sawtooth does not require accessing Customer's survey data, and the data will remain confidential as Sawtooth Customer policy states. Thus, Sawtooth collects, transfers, manages, and stores Customer's survey without knowing the content of the data that is being Processes. However, Sawtooth acknowledges that, in the course of the performance of the Services, it may be exposed to personally identifiable information in the survey data as part of query logs that are passed to it from Customer's data infrastructure environment or through other search or data sampling functionality that Customer initiates within the Sawtooth system. To the extent that any such personal data is passed to Sawtooth, Sawtooth Processes and utilizes such data only for the sole purpose of trouble shooting or performing specific requested services by Customer, and not for any other purpose.

Purpose(s) of the Data Transfer and Further Processing:
The purposes of the data transfer are to (1) move the survey data from one country where the Survey Respondents are to another country where the survey data can be stored in the data center (the US by default); (2) send the data back from the country where the data center is to where the Software is being used by Customer's authorized user for analysis. In other words, the location of the data center determines where the data is stored; where the Survey Respondents are is the location of data collection; and the physical location of the Customer's authorized users of the software determines the where the analysis occurs. Thus, if and when the data center location is in a country (the US by default) different from the country where the software is being utilized by Customer's authorized user, data transfer is required for (1) Cloud storage and (2) analysis. If and when the survey respondent's location at the time of survey collection is in a country different from the data center (the US by default), data transfer shall occur.

The Period for Which the Survey Data Will be Retained, or, If That is Not Possible, the Criteria Used to Determine that Period:
The duration of data retention is (1) until the expiration of the subscription plus 90 days in the Processor's backup system; (2) until Controller terminates the subscription plus 90 days in the Processor's backup system; (3) until Customer deletes Customer Data plus 90 days in the Processor's backup system; or (4)

until Data Subject requests erasure of his or her personal information plus 90 days in the Processor's backup system.

For Transfers to (Sub-) Processors, Also Specify Subject Matter, Nature, and Duration of the Processing:

1. The transfers to Processor.

a. Subject matter: Customer engages Processor's web hosting services and utilizes Processor's data infrastructure in the cloud to continuously store, access, and manage Customer's survey data.

b. Nature: for storing and managing survey data in the web hosting environment.

c. Duration: (1) until the expiration of the subscription; (2) until Customer terminates the subscription; (3) until Customer deletes Customer Data; or (4) until Data Subject requests erasure of his or her personal information.

2. The transfers to Sub-processor.

a. Subject matter: Processor engages Sub-processor's cloud services to build Customer's hosting environment and utilizes Sub-processor's data center to store Customer's survey data.

b. Nature: for storing and transferring Customer's survey data in the cloud.

c. Duration: (1) until the expiration of the subscription; (2) until Customer terminates the subscription; (3) until Customer deletes Customer Data; or (4) until Data Subject requests erasure of his or her personal information.

C. COMPETENT SUPERVISORY AUTHORITY FOR MODULE TWO (i.e., transfer controller to Processor) AND MODULE FOUR (i.e., transfer processor to controller).

I. Identify the competent supervisory authority/ies pursuant to Clause 13.

1. Supervisory Authority Contact Information in _____ (The location of majority of Customer's Survey Respondents):
   a. Name:
   b. Address:
   c. Phone:
   d. Website:

ANNEX II

A. TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA FOR MODULE TWO (i.e., transfer controller to Processor) AND MODULE FOUR (i.e., transfer processor to controller).

a. Overview: Sawtooth will implement and maintain a written information security program that maintains administrative, technical, and physical safeguards, designed to:

(i) Provide the security and confidentiality of all Confidential Information that is Processed, stored, or controlled by Sawtooth;

(ii) Protect against anticipated threats or hazards to the security or integrity of such Confidential Information;

(iii) Prevent unauthorized access to or loss, acquisition, disclosure, or use of such Confidential Information; and

(iv) Provide the secure disposal of Confidential Information in compliance with applicable standards.

b. Sawtooth will use reasonable efforts to abide by its written information security program and administrative, technical, and physical safeguards align with accepted industry practices and comply with applicable data protection and privacy laws, as well as the terms and conditions in Sawtooth's Information Security Policy.

Restrictions or safeguards

1. The nature of the Customer Data that Sawtooth permits to Process is considered as either pseudonymous or with identifiers.
2. The risks involved for Processing the data is considered low.
3. Sawtooth policy restricts the sales of any personal information or proprietary information of another and physical and cyber access of Customer's projects and data unless an individual is authorized by both Customer and Sawtooth.
4. Sawtooth policy prohibits unauthorized personnel to access Customer's files and applications.
5. Sawtooth policy requires employees to have a unique, secure password that changes every year for the work laptop/computer.
6. Sawtooth sets log out timer on every Customer laptop with control disabled.
7. Sawtooth policy requires and monitors monthly security trainings of all employees.
8. Sawtooth policy requires contacting Customer within 72 hours in the event of data breach.
9. All entrances to the office are automatically locked and require authorized key card for access.
10. Sawtooth requires the entire office security system to be armed during hours of non-operation.
11. Sawtooth requires only using Processors/Sub-processors that are in compliance with the security, data protection, and privacy laws and regulations and equipped with relevant certifications.
12. Sawtooth requires security applications installed in every work computer/laptop to monitor and prevent cyber-attacks and computer viruses.
13. Sawtooth only uses sub-processors that implement:
    - Measures of pseudonymisation and encryption of personal data
    - Measures for ensuring ongoing confidentiality, integrity, availability and resilience of Processing systems and services
    - 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 Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the Processing

- Measures for user identification and authorisation
- Measures for the protection of data during transmission
- Measures for the protection of data during storage
- Measures for ensuring physical security of locations at which personal data are Processed
- Measures for ensuring events logging
- Measures for ensuring system configuration, including default configuration
- Measures for internal IT and IT security governance and management
- Measures for certification/assurance of Processes and product
- Measures for ensuring data minimisation
- Measures for ensuring data quality
- Measures for ensuring limited data retention
- Measures for ensuring accountability
- Measures for allowing data portability and ensuring erasure

Information Security Policy

The data Processor will maintain a documented and up-to-date security policy that all employees and subcontractors are to be made aware of and comply with.

Organizational Information Security

The data Processor will have an organized, formal information security program that includes the following components:

(i) Criminal background checks are in place for all employees who have access to data.
(ii) Regular training of all staff on information security principles.
(iii) An individual at board-level or higher designated as the officer responsible for the Customer's information security strategy and its implementation.
(iv) Classification levels for all Customer, and all Customer Data are classified as confidential.

Physical/Environmental Security

The Data Processor will ensure a secure working environment where all data will be Processed, stored, or consumed. This environment must provide reasonable coverage to mitigate or eliminate risks including, but not limited to:

(i) Fires, floods, earthquakes, and other natural disasters.
(ii) Operational disturbance (such as power, internet, or other service outages).
(iii) Theft and/or any unauthorized access.

Access Control

The Data Processor will keep a formal access control Process & policy in place for system(s) on which data will be Processed, stored, transferred, or consumed. This access control Process & policy will incorporate the following principles:

(i) Role-Based Access control for administrators as well as users.
(ii) Privileges granted on a principle of least-privilege.
(iii) Access is protected according to industry-standard best practices (password policies and etc. are strictly followed and updated regularly).
(iv) Access is given only on a "need-to-know" basis.

Service Management

The services the data importer provides will adhere to the following security principles:

(i) Sufficient measures will be provided to ensure the integrity and availability of the service as specified in the service's published Terms of Use.

(ii) Data in motion between the data importer's systems and the data exporter's systems will be encrypted by default according to current industry-standard encryption Processes (such as TLS).
(iii) Data at rest on the Data Processor's systems must be encrypted according to current industry-standard encryption Processes.
(iv) Policies and procedures must be maintained and followed to ensure any services built by the data Processor are protected from common security vulnerabilities.

Incident Management

The Data Processor will maintain the following documentation related to incident management:
(i) A Business Continuity Plan (BCP) must be maintained to ensure a restoration of services after any interruption of service.
(ii) The Data Processor will test aspects of the BCP regularly to verify that the Processes are up-to-date and feasible in the case of disaster.
(iii) The Data Processor will maintain incident management procedures to quickly respond to and mitigate incidents that might impact data owned by the data controller.
(iv) The Data Processor will notify the data controller within 72 hours of security incident(s) that impact the data owned by the data controller.

ANNEX III

A. LIST OF SUB-PROCESSORS - MODULE TWO (i.e., transfer controller to Processor).

EXPLANTORY NOTE:
This Annex must be completed for Modules Two and Three in the case of the specific authorization of sub-processors (Clause 9(a), Option 1).

1. The controller has authorized the use of the following sub-processors:

    a. Sub-processors Contact Information

Name: Rackspace Technology
Address: 1 Fanatical Pl, Windcrest, TX 78218, USA
Contact: Data Protection Officer
Position: DPO
Email: privacy@rackspace.com

Name: Amazon Web Services
Address: 410 Terry Avenue North Seattle, WA 98109, USA
Contact: AWS Compliance Reports Support - Amazon Web Services
Email: aws-EU-privacy@amazon.com

Name: Microsoft Azure
Address: One Microsoft Way, Redmond, Washington, USA
Contact: Microsoft-Report a Privacy Concern
Email: dpoffice@microsoft.com

Name: Stova
Address: 13 Marshall Street, Suite One, Norwalk, CT 06854
Contact: Data Protection Officer
Position: DPO
Email: privacy@stova.io.

Name: Salesforce
Address: 415 Mission Street, 3rd Floor, San Francisco, CA 94105
Contact: Data Protection Officer
Position: DPO
Email: privacy@salesforce.com

Name: Oracle NetSuite
Address: 2300 Oracle Way, Austin, TX 78741
Contact: Data Protection Officer
Position: DPO
Email: Infonetsuite_WW@oracle.com

Name: DocuSign
Address: 221 Main St., Suite 1550, San Francisco, CA 94105
Contact: Data Protection Officer
Position: DPO
Email: privacy@docusign.com

Name: Bettermode
Address: 22 Wellesley St E, Toronto, Ontario, Canada
Contact: Data Protection Officer
Position: DPO

Email: dpo@bettermode.com

b. Description of Processing.

i. Providing cloud storage.
ii. Facilitating cloud migration.

2. In addition to the sub-processors listed above, the following entity is a subsidiary of Sawtooth Software Inc., and accordingly may also function as a sub-processor.

a. Sub-processors Contact Information

Name: Sawtooth Software UK Ltd.
Address: C/O Monetta Llp, 232 Stamford Street Central, Ashton-Under-Lyne, United Kingdom, OL6 7NQ
Contact: Data Protection Officer
Position: DPO
Email: dpo@sawtoothsoftware.com

b. Description of Processing.

i. B2B Customer employees' personal data sharing and transferring.
ii. B2B Customer/technical support that may or may not access Customer Survey Respondents' data depending on the needs of the Customer.

APPENDIX 2

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

As permitted by clause 17 of this Addendum, the parties agree to change the format of the information set out in Part 1 of the Addendum such that:

a. For the purposes of Table 1, Sawtooth shall be the "importer" and Customer shall be the "exporter" with the applicable details the same as identified in the Agreement.

b. For the purposes of Table 2, the version of the Approved EU SCCs which this Addendum is appended to, set forth in Appendix 1-A, including the Annexes in Appendix 1-B shall apply.

c. For purposes of Table 3, Annex I.A and Annex I.B in Appendix 1-B will be deemed completed with the information set forth in Annex I to Appendix 1-B, Annex II will be deemed completed with the information set forth in Annex II to Appendix 1-B, and Annex III will be deemed completed with the information set forth in Annex III to Appendix 1-B.

d. For purposes of Table 4, neither party may terminate this Addendum when the Approved Addendum changes.

Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows Data Subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum Incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs, which this Addendum is appended to, as set out in Table 2, including the Appendix 1-B Information.
Appendix Information	As set out in Table 3.

Appropriate Safeguards	The standard of protection over the personal data and of Data Subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementation Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the Processing of personal data, privacy, and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU

SCCs provides greater protection for Data Subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:
       "and, with respect to data transfers from controllers to Processors and/or Processors to Processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

    c. Clause 6 (Description of the transfer(s)) is replaced with:
       "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I where UK Data Protection Laws apply to the data exporter's Processing when making that transfer";

    d. Clause 8.7(i) of Module 1 is replaced with:
       "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

    e. Clause 8.8(i) of Modules 2 and 3 is replaced with:
       "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

    f. References to "Regulation (EU) 2016/679," "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)," and "that Regulation" are all replaced by "UK Data Protection Laws." References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union," "Union," "EU," "EU Member State," "Member State," and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with: "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply";

m. Clause 17 is replaced with: "These Clauses are governed by the laws of England and Wales";

n. Clause 18 is replaced with: "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A Data Subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts"; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

    b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix 1-B Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes," will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in (a) its direct costs of performing its obligations under the Addendum; and/or (b) its risk under the Addendum, and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.