Exhibit A to the Master Subscription Agreement

DATA PROCESSING ADDENDUM

This DATA PROCESSING ADDENDUM ("**DPA**") forms part of the Master Service Agreement (the "**Agreement**") between: (i) **Company**, acting on its own behalf; and (ii) **Customer** acting on its own behalf (Company and Customer will together be referred to as the "Parties"). This DPA shall be effective as of the last signature in the Agreement.

The terms used in this DPA shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

1. Definitions

1.1. In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1. "**Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Company, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.2. "**CCPA**" means the California Consumer Privacy Act of 2018, California Civil Code Section 1798.100, *et seq.*, as amended by the California Privacy Rights Act of 2020 ("CPRA"), and its implementing regulations adopted by the California Attorney General and/or the California Privacy Protection Agency;

1.1.3. "**Data Breach**" means a breach of security leading to the accidental, unauthorized, or unlawful destruction, loss, alteration, disclosure of, access to, or other Processing of Personal Data transmitted, stored, or otherwise Processed;

1.1.4. "**Data Protection Laws**" means all data protection laws and regulations applicable to a Party's Processing of Personal Data under the Agreement, including, where applicable, EU Data Protection Laws, the CCPA and other applicable State Privacy Laws;

1.1.5. "**Data Subject Request**" means a request made by a Data Subject in accordance with the rights granted under Data Protection Laws, including but not limited to requests to know, delete and opt-out under the CCPA and requests to access, rectify, erase, restrict Processing, data portability, object to Processing and not to be subject to automated individual decision making under EU Data Protection Laws;

1.1.6. "**EU Data Protection Laws**" means all data protection laws and regulations applicable to Europe, including, as applicable: (i) GDPR; (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the

electronic communications sector (the "ePrivacy Directive"); (iii) U.K. GDPR and (v) in respect of Switzerland, the revised Federal Act on Data Protection of 1 September 2023 ("revFADP");

1.1.7. **"Europe"** means the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom;

1.1.8. "**EU Standard Contractual Clauses**" means the contractual clauses set out in the Annex to Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, amended as indicated in Section 6 of Annex B to this DPA;

1.1.9. **"GDPR"** means regulation 2016/679 of the European Parliament and of the Council 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).

1.1.10. "**Personal Data**" means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with an identified or identifiable natural person or particular household;

1.1.11. "**Process**" or "**Processing**" means any operation or set of operations which is performed on Personal Data by Company or its Subprocessors, or in connection with and for the purposes of the provision of the Services, whether or not accomplished by automatic means, including but not limited to 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; and as defined by Data Protection Laws;

1.1.12. "**Sensitive Data**" means (a) social security number, tax file number, passport number, driver's license number, or similar identifier (or any portion thereof); (b) credit or debit card number (other than the truncated (last four digits) of a credit or debit card); (c) employment, financial, credit, genetic, biometric or health information; (d) racial, ethnic, political or religious affiliation, trade union membership, information about sexual life or sexual orientation, or criminal record; (e) account passwords; or (f) other information that falls within the definition of "special categories of data" or "special personal information" under applicable Data Protection Laws;

1.1.13. "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of Company for Customer pursuant to the Agreement;

1.1.14. **"State Privacy Laws"** means the privacy laws of the states of the United States of America, including but not limited to the CCPA, the Colorado Privacy Act, the Connecticut Data Privacy Act, the Delaware Personal Data Privacy Act, the Indiana Consumer Data Protection Act, the Iowa Consumer Data Protection Act, the Kentucky Consumer Data Protection Act, the Maryland Online Data Privacy Act, the Minnesota Consumer Data Privacy Act, the Montana Consumer Data Privacy Act, the Nebraska Data Privacy Act, the New Hampshire Data Privacy Act, the New

Jersey Privacy Act, the Oregon Consumer Privacy Act, the Rhode Island Data Transparency and Privacy Protection Act, the Tennessee Information Protection Act, the Texas Data Privacy and Security Act, the Utah Consumer Privacy Act, and the Virginia Consumer Data Protection Act, and all of their implementing regulations.

1.1.15. "**U.K. GDPR**" means the GDPR as implemented by the United Kingdom pursuant to the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 and any other data protection and security related laws applicable in the UK;

1.1.16. "**U.K. Standard Contractual Clauses**" means the International Data Transfer Addendum to the EU Standard Contractual Clauses for the transfer of personal data from controllers to processors established in third countries which do not ensure an adequate level of protection, as approved by the UK Information Commissioner's Office (ICO).

1.1.17. The terms, "**Commission**", **"Contractor",** "**Controller**", "**Data Subject**", "**Member State**", "**Processor**", **"Service Provider", "Subprocessor"**, and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

1.1.18. The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. Processing of Personal Data.

2.1. Roles of the Parties. The Parties acknowledge and agree that with respect to the Processing of Personal Data under the Agreement, Customer is the Controller or Processor, and Company is the Processor or Subprocessor and, where applicable under State Privacy Laws, a Service Provider or Contractor. The subject matter, duration, purpose of the Processing, and types of Personal Data and categories of Data Subjects under this DPA are set forth in Annex A.

2.2. Customer Obligations. Customer represents and warrants that (i) it has complied, and will continue to comply, with all applicable laws, including Data Protection Laws, in respect of its Processing of Personal Data and any processing instructions it issues to Company; and (ii) it has provided, and will continue to provide, all notice and has obtained, and will continue to obtain, all consents and rights necessary under Data Protection Laws for Company to Process Personal Data for the purposes described in the Agreement. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Without prejudice to the generality of the foregoing, Customer agrees that it shall be responsible for complying with all laws (including Data Protection Laws) applicable to any content created, sent or managed through the Services.

2.3. Company's Obligations. Company will comply with applicable Data Protection Laws in Processing Personal Data. Company will Process Personal Data only in accordance with Customer's documented written instructions. The Parties agree that the Agreement (including this DPA) sets out Customer's complete and final instructions to Company in relation to the Processing of Personal Data, and processing outside of the scope of these instructions (if any) shall require prior written agreement of both of the Parties.

2.4. **Lawfulness of Customer's Instructions**. Customer shall ensure that Company's processing of Personal Data in accordance with Customer's instructions will not cause Company to violate any applicable law, regulation, or rule, including, without limitation, Data Protection Laws.

2.5. **Details of the Processing**. The subject-matter of the Processing of Personal Data by Company is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Annex A hereto.

3. Subprocessing.

3.1. **General Authorization.** Customer generally authorizes the use of Subprocessors to Process Personal Data in connection with fulfilling Company's obligations under the Agreement and/or this DPA. A list of current Subprocessors can be viewed at https://www.polytomic.com/privacy-policy#service-providers (the "Subprocessor List"). Customer hereby authorizes Company to engage the Subprocessors listed in the Subprocessor List. Any appointment of a further Subprocessor must comply with: (a) Section 2.5 of the Agreement; and (b) Annex B and/or Annex C, to the extent applicable to Personal Data subject to EU Data Protection Laws or State Privacy Laws. For the avoidance of doubt, the same requirements shall apply to Personal Data from any other jurisdiction where required by applicable Data Protection Laws.

3.2. **Communication With Subprocessors.** Customer shall not directly communicate with Company's Subprocessors about the Services, unless agreed to in writing by Company in Company's sole discretion.

4. Security.

4.1. **Company's Personnel**. Company shall ensure that any person who is authorized by Company to process Personal Data (including its staff and agents) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

4.2. **Security Measures.** Company shall implement and maintain commercially reasonable technical and organisational measures that are designed to protect against Data Breaches involving, and unauthorized or accidental destruction, loss, alteration or damage, unauthorized disclosure of or access to, Personal Data and designed to preserve the security and confidentiality of Personal Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, in accordance with the security standards described in Annex D (the "**Security Measures**").

4.3. **Updates to Security Measures.** Customer acknowledges that the Security Measures are subject to technical progress and development and that Company may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Services provided to Customer.

4.4. **Customer's Obligations Regarding Security Measures.** Customer is responsible for independently determining whether the Security Measures adequately meet its obligations under applicable Data Protection Laws. Customer is also responsible for its secure use of the Services, including protecting the security of Personal Data in transit to and from the Services (including securely backing up or encrypting any such Personal Data).

5. Data Breach.

5.1. Notification. In the event that Company becomes reasonably aware of any Data Breach, Company will use good faith efforts to notify Customer of the Data Breach without undue delay, but in no event later than seventy-two (72) hours after Company becomes reasonably aware of the Data Breach. The notification obligations in this Section 5 do not apply to incidents that are caused by Customer or Customer's personnel or users or to unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewall or networked systems.

5.2. Manner of Notification. Notification of a Data Breach, if any, will be delivered to one or more of Customer's business, technical or administrative contacts by any means that Company selects, including via electronic mail. It is Customer's sole responsibility to ensure that it maintains accurate contact information with Company at all times.

5.3. Data Breach Management. Company shall make commercially reasonable efforts to identify the cause of a Data Breach and take those steps that Company deems necessary and reasonable to remediate the cause of such Data Breach to the extent that remediation is within Company's reasonable control.

6. Termination.

6.1. Termination. This DPA shall terminate automatically upon the later of (a) the termination or expiry of the Agreement, or(b) Company's deletion or return of the Personal Data to Customer.

6.2. Return or Deletion of Data. Upon termination or expiration of this DPA, Company shall (at Customer's election) delete or return to Customer all existing copies of Personal Data, unless Data Protection Laws require continued retention of the Personal Data. Upon Customer's request, Company shall confirm compliance with these obligations in writing. This requirement shall not apply to Personal Data that Company has archived on backup systems, which Personal Data shall be deleted by Company at such time as Company next restores to its active systems the backup that contains the Personal Data.

7. Data Subject Requests.

7.1. Data Subject Requests. In the event that a Data Subject Request is made to Company, Company shall not respond to the Data Subject Request directly, except to direct the Data Subject to contact Customer directly or as required by Data Protection Laws. If Company is required by Data Protection Laws to respond to the Data Subject Request, it shall notify Customer by any means that Company selects, including via electronic mail, unless prohibited from doing so by Data Protection Laws. For the avoidance of doubt, nothing in the Agreement or the DPA shall restrict or prevent Company from responding to any Data Subject Request or request or inquiry from a Data Protection Authority in relation to Personal Data for which Company is a Controller.

8. Jurisdiction Specific Terms.

8.1. To the extent that Company Processes Personal Data subject to EU Data Protection Laws, the terms of Annex B shall apply and are hereby incorporated into the DPA by this reference. To

the extent that Company Processes Personal Data subject to the State Privacy Laws, the terms of Annex C shall apply and are hereby incorporated into the DPA by this reference.

9. Limitation of Liability.

9.1. **Limitation of Liability.** To the extent permitted by applicable Data Protection Laws, each Party's (and all of that Party's Affiliates') liability taken together in the aggregate arising out of or related to this DPA (including the SCCs) shall be subject to the exclusions and limitations of liability set forth in the Agreement.

9.2. **Claims by Customer.** Any claims made against Company or its Affiliates under or in connection with this DPA (including, where applicable, the SCCs) shall be brought solely by the Customer entity that is a party to the Agreement.

9.3. **Exclusion.** In no event shall any Party limit its liability with respect to any individual's data protection rights under this DPA or otherwise.

10. Concluding Provisions

10.1. **Amendments**. This DPA may not be amended or supplemented, nor shall any of its provisions be deemed to be waived or otherwise modified, except through a writing duly executed by authorized representatives of Company and Customer.

10.2. **Severability**. Should any provision of this DPA or any of the Annexes be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained herein.

10.3. **Governing Law**. This DPA will be governed by and construed in accordance with the laws of the jurisdiction selected in the Agreement, without regard to conflict of laws provisions, unless required otherwise by Data Protection Laws.

10.4. **Notice**. Any notices that are required to be provided in this DPA shall be provided in accordance with any notice provision of the Agreement, unless otherwise specified.

ANNEX A TO DPA

DESCRIPTION OF THE PROCESSING

1. Subject Matter and Details of the Processing

The Parties acknowledge and agree that (i) the subject matter of the Processing under the Agreement is Company's provision of the Services; (ii) the duration of the Processing is from Company's receipt of Personal Data until deletion or return of all Personal Data by Company in accordance with the Agreement and this DPA; (iii) the nature and purpose of the Processing is to provide the Services; (iv) the Data Subjects to whom the Personal Data pertains are Customer's end users; and (v) the categories of Personal Data can include email addresses, phone numbers, physical addresses, or any other categories Customer transfers using the Company product.

2. Types of Personal Data

- Email addresses
- Phone numbers
- Physical addresses
- Other types that Customer chooses to transfer using the Company product

3. Categories of Data Subjects

- Customer's end users
- Other categories that Customer chooses to transfer using the Company product

4. Categories of Sensitive Data

None.

5. Obligations and Rights of the Controller

The obligations and rights of Customer are as set out in the Agreement and the DPA.

6. Duration of the Processing.

The duration of the Processing shall be during the term of the Agreement.

ANNEX B TO DPA

PROVISIONS APPLICABLE TO PROCESSING OF PERSONAL DATA SUBJECT TO EU DATA PROTECTION LAWS

The provisions of this Annex B will apply to the Processing by Company of Personal Data under the Agreement, but only to the extent that the Processing of Personal Data is subject to EU Data Protection Laws. In the event of any conflict between the provisions of this Annex B and the DPA or the Agreement, the provisions of this Annex B shall control.

1. **Processing of Personal Data.**

1.1. **Roles of the Parties.** When Processing Personal Data that is subject to EU Data Protection Law in accordance with Customer's instructions, the Parties acknowledge that Customer is the Controller of the Personal Data and Company is the Processor.

1.2. **Legality of Processing Instructions.** Company shall inform Customer in writing, including by electronic mail, if it believes that an instruction of Customer relating to the Processing of Personal Data infringes on EU Data Protection Laws.

2. Subprocessors.

2.1. **Objection to New Subprocessors**. If Customer has a reasonable objection to the addition of a new Subprocessor to the Subprocessor List in accordance with Section 3.1 of the DPA, Customer must notify Company of the objection in writing within ten (10) calendar days of the addition of the new Subprocessor to the Subprocessor List. If Customer does not notify Company in writing of an objection within ten (10) calendar days, Customer waives any objection that it may have had to the new Subprocessor. If Customer submits an objection in accordance with this Section 2, the Parties agree to discuss Customer's concerns in good faith with a view toward achieving a commercially reasonable resolution. If no such resolution can be reached within thirty (30) calendar days, Company may, at its option, either (a) withdraw the objectionable Subprocessor and either perform the Services itself, or appoint a new Subprocessor in accordance with the terms of Section 3.1 of the DPA, or (b) permit Customer to suspend or terminate the Services and the Agreement in accordance with the termination provisions of the Agreement without liability to either party (but Customer must pay any fees incurred for Services actually performed by Company prior to suspension or termination in accordance with the terms of the Agreement). The parties agree that by complying with this Section 2, Company fulfills its obligations under Section 9 of the Standard Contractual Clauses.

2.1.1. **Subprocessor Contractual Terms.** Company will contractually impose data protection obligations on its Subprocessors that are equivalent to those data protection obligations imposed on Company under the DPA and this Annex B.

2.1.2. **Liability for Acts/Omissions of Subprocessors.** Company shall remain liable for the acts and omissions of its Subprocessors to the same extent that Company would be liable if it performed the services of each Subprocessor directly under the terms of this DPA.

3. **Data Subject Requests.** Taking into account the nature of the Processing, Company shall assist Customer by appropriate technical and organisational measures, insofar as it is possible, for the fulfillment of Customer's obligation to respond to a Data Subject Request.

4. **Data Protection Impact Assessment.** To the extent required under applicable Data Protection Laws, Company shall (taking into account the nature of the processing and the information available to Company) provide all reasonably requested information regarding the Services to enable Customer to carry out data protection impact assessments or prior consultations with Supervisory Authorities as required by Data Protection Laws. Company shall comply with the foregoing by: (i) complying with Section 5 (Audits) of this Annex B; (ii) providing the information contained in the Agreement, including this DPA; and (iii) if the foregoing subsections (i) and (ii) are insufficient for Customer to comply with such obligations, upon request, providing additional reasonable assistance (at Customer's expense).

5. Audits.

5.1. **Audits Generally.** Company will make information reasonably necessary to demonstrate compliance with this DPA available to Customer. Customer may audit Company's compliance with its obligations under this DPA up to once per year and on such other occasions as may be required by applicable Data Protection Laws, including where mandated by Customer's Supervisory Authority. Any audit must be conducted during regular business hours, subject to the agreed final audit plan as set forth in Section 5.3 of this Annex B and subject to Company's safety, security or other relevant policies, and may not unreasonably interfere with Company's business activities.

5.2. **Third Party Auditors.** If a **third** party is to conduct an audit under Section 5.1 of this Annex B, Company may object to the auditor if the auditor is, in Company's reasonable opinion, a competitor of Company. Such objection by Company will require Customer to appoint another auditor or conduct the audit itself. Customer will be responsible for all fees charged by any auditor appointed by Customer to execute any audit under this Section 5.

5.3. **Audit Plan.** Aside from an audit of a **Supervisory** Authority, to request an audit, Customer must submit a detailed proposed audit plan to Company at least thirty (30) calendar days in advance of the proposed audit date and any third party auditor must sign a customary non-disclosure agreement mutually acceptable to the Parties (such acceptance not to be unreasonably withheld) providing for the confidential treatment of all information exchanged in connection with the audit and any reports regarding the results or findings thereof. The proposed audit plan must describe the scope, duration and start date of the audit. Company will review the proposed audit plan and provide Customer with any concerns or questions (for example, any request for information that could compromise Company's security, privacy, employment or other relevant policies). Company will work cooperatively with Customer to agree on a final audit plan. Nothing in this Section 5.3 shall require Company to disclose any information where such disclosure would result in a breach of any duty of confidentiality.

5.4. **Third Party Audit Reports.** If the controls or measures to be assessed in the requested audit are addressed in an SOC 2 Type 2, ISO, NIST or similar audit report performed by a qualified third party auditor within twelve (12) months of Customer's audit request and Company has confirmed there are no known material changes in the controls audited, Customer agrees to accept such report in lieu of requesting an audit of such controls or measures.

5.5. **Subprocessor Information.** Nothing in this Section 5 shall be construed to require Company to furnish more information about its Subprocessors in connection with such audits than such Subprocessors make available to Company without restriction on further disclosure.

5.6. **Audit Reports.** Customer will promptly notify Company of any non-compliance discovered during the course of an audit and provide Company any audit reports generated in connection with any audit under this Section 5 unless prohibited by applicable Data Protection Laws or otherwise instructed by a Supervisory Authority. Customer may use the audit reports only for the purposes of meeting Customer's regulatory audit requirements and/or confirming compliance with the requirements of this DPA. If any audit reveals that Company is not in compliance with the provisions of this DPA and/or applicable Data Protection Laws, Company shall take commercially reasonable corrective actions including temporary work-arounds reasonably necessary to comply with the provisions of this DPA and/or applicable Data Protection Laws.

6. Cross-Border Data Transfers.

6.1. **Processing in the United States.** Customer acknowledges that, as of the date of this DPA, Company's primary Processing facilities are located in the United States of America.

6.2. **EU Standard Contractual Clauses:** For data transfers from the European Economic Area to a country that has not been deemed by the European Commission to provide an adequate level of protection of Personal Data pursuant to Article 45 of the GDPR, Module Two and/or Module Three (as applicable) of the EU Standard Contractual Clauses will apply in the following manner:

6.2.1. In Clause 7, the optional docking clause will not apply;

6.2.2. In Clause 9(a), Option 2 will apply, and the time period for notice of Subprocessor changes will be as set forth in Section 3 (Subprocessing) of the DPA;

6.2.3. In Clause 11, the optional language will not apply;

6.2.4. In Clause 17, Option 1 will apply, and the EU Standard Contractual Clauses will be governed by Irish law;

6.2.5. In Clause 18(b), disputes will be resolved before the courts of Ireland;

6.2.6. In Annex 1, Part A:

6.2.6.1. Data Exporter: Customer and authorized affiliates of Customer;

6.2.6.2. Contact Details: Customer's email address, or the email address(es) for which Customer elects to receive privacy communications.

6.2.6.3. Data Exporter Role: The Data Exporter's role is defined in Section 2 of this DPA.

6.2.6.4. Signature & Date: By entering into this DPA, Data Exporter is deemed to have signed the EU Standard Contractual Clauses (Module 2 and/or Module 3, as applicable) incorporated herein, including their Annexes, as of the date of this DPA.

6.2.6.5. Data Importer: Polytomic Inc.

6.2.6.6. Contact Details: contact@polytomic.com

6.2.6.7. Data Importer Role: The Data Importer's role is outlined in Section 2 of this DPA.

6.2.6.8. Signature & Date: By entering into this DPA, Data Importer is deemed to have signed the EU Standard Contractual Clauses (Module 2 and Module 3) incorporated herein, including their Annexes, as of the date of this DPA.

6.2.7. In Annex I, Part B:

6.2.7.1. The categories of Data Subjects are described in Annex A, Section 3 to this DPA.

6.2.7.2. The Sensitive Data transferred is described in Annex A, Section 4 to this DPA.

6.2.7.3. The frequency of the transfer is a continuous basis for the duration of the Agreement.

6.2.7.4. The nature of the processing is described in Annex A, Section 1 to this DPA.

6.2.7.5. The purpose of the processing is described in Annex A, Section 1 to this DPA.

6.2.7.6. The period of the processing is described in Annex A, Section 1 to this DPA.

6.2.7.7. For transfers to Subprocessors, the subject matter of the processing is as outlined in https://www.polytomic.com/privacy-policy#service-providers.

6.2.7.8. For transfers to Subprocessors, the nature of the processing is as outlined in https://www.polytomic.com/privacy-policy#service-providers.

6.2.7.9. For transfers to Subprocessors, the duration of the processing is as outlined in https://www.polytomic.com/privacy-policy#service-providers.

6.2.8. In Annex I, Part C, the competent Supervisory Authority shall be determined in accordance with Clause 13 of the EU Standard Contractual Clauses.

6.2.9. Annex D to this DPA serves as Annex II to the EU Standard Contractual Clauses.

6.3. **U.K. Standard Contractual Clauses:** For data transfers from the United Kingdom to a country that has not been deemed by the United Kingdom Information Commissioner's Office to provide an adequate level of protection of Personal Data pursuant to Article 45 of the U.K. GDPR, the U.K. Standard Contractual Clauses will apply in the following manner:

6.3.1. The illustrative indemnification clause will not apply;

6.3.2. The selected option in Section 6.2 of this Annex B shall apply, mutatis mutandis, to the extent compatible with the UK Addendum;

6.3.3. Annex A serves as Appendix 1 to the U.K. Standard Contractual Clauses; and

6.3.4. Annex D serves as Appendix 2 to the U.K. Standard Contractual Clauses.

6.4. **Swiss Transfers**: For data transfers from Switzerland to a country that has not been recognised as providing an adequate level of protection under the revFADP, the EU Standard Contractual Clauses shall apply with the modifications required under Swiss law, including that references to the GDPR shall, where required, be interpreted as references to the revFADP, references to "Member State" shall include Switzerland, the Swiss Federal Data Protection and Information Commissioner shall be the competent authority where required, and Swiss data subjects may exercise their rights in Switzerland.

6.5. **Conflicts.** To the extent there is any conflict between the EU Standard Contractual Clauses or the U.K. Standard Contractual Clauses and any other terms in this DPA, including Section 8.1 (Jurisdiction Specific Terms), the provisions of the EU Standard Contractual Clauses and/or U.K. Standard Contractual Clauses will prevail, but only to the extent that the EU Standard Contractual Clauses and/or the U.K. Standard Contractual Clauses apply.

6.6. **Amendments to EU Standard Contractual Clauses or U.K. Standard Contractual Clauses or Swiss Transfer provisions**. If the European Commission, the United Kingdom Information Commissioner's Office or the Swiss Federal Data Protection and Information Commissioner or another competent Supervisory Authority amends or replaces the EU Standard Contractual Clauses or the U.K. Standard Contractual Clauses or other applicable transfer provisions, the parties shall promptly discuss the proposed amendments and negotiate in good faith with a view toward agreeing and implementing those amendments or updates as soon as is reasonably practicable.

ANNEX C TO DPA

PROVISIONS APPLICABLE TO PROCESSING OF PERSONAL DATA SUBJECT TO STATE PRIVACY LAWS

The provisions of this Annex C will apply to the Processing by Company of Personal Data under the Agreement, but only to the extent that the Processing of Personal Data is subject to State Privacy Laws. In the event of any conflict between the provisions of this Annex C and the DPA or the Agreement, the provisions of this Annex C shall control.

1. **Definitions.** As used in this Annex C, the terms "**Business Purpose**", "**Personal Information**", "**Sale**" and "**Service Provider**" shall have the same meaning as in the CCPA (California Civil Code Section 1798.140), and their cognate terms shall be construed accordingly.

2. **Types of Personal Data.** The personal data that Company Processes on behalf of Customer is listed in Annex A to this DPA.

3. **Duration of the Processing.** The duration of the processing is listed in Annex A to this DPA.

4. **Roles of the Parties.** The Parties acknowledge and agree that, with regard to the Processing of Personal Data that constitutes Personal Information performed solely on behalf of Customer, Company is a Service Provider or Contractor and receives Personal Information pursuant to the Business Purpose of performing services on behalf of Customer, providing the services referenced in the Agreement, including helping Customer to sync data between systems. Customer is disclosing personal information to Company only for the limited and specified business purpose of providing the Services.

5. **No Sale of Personal Data to Company.** Customer and Company hereby acknowledge and agree that in no event shall the transfer of Personal Data that constitutes Personal Information from Customer to Company pursuant to the Agreement constitute a Sale of Personal Information to Company, and that nothing in the Agreement shall be construed as providing for the Sale of Personal Information. The Parties acknowledge and agree that Company's access to Personal Data that constitutes Personal Information does not constitute part of the consideration exchanged by the Parties in respect of the Agreement.

6. **Limitations on Use and Disclosure.** Company will not sell or share the Personal Data Processed under this DPA and will not retain, use or disclose the Personal Data for any purposes other than the specific purpose of performing the Services as provided in the Agreement, the Business Purposes specified in the Agreement, and as required under State Privacy Laws. Company shall not retain, use or disclose Personal Data outside of the direct business relationship between Company and Customer. Company hereby certifies that it understands the foregoing restrictions and will comply with them in accordance with the requirements of State Privacy Laws, including but not limited to the CCPA.

7. **Service Providers/Subprocessors.** To the extent that Company discloses Personal Data received from Customer pursuant to this DPA to Service Providers/Subprocessors, Company shall enter into a written agreement with the Service Provider/Subprocessor that requires the Service Provider/Subprocessor to meet the same obligations that this DPA imposes upon Company. To the extent that the Processing is subject to the Colorado Privacy Act, the Delaware Personal Data Privacy Act, the Minnesota Consumer Data Privacy Act, or the New Hampshire Data Privacy Act or other State Privacy Laws (to the extend required), the parties

agree that the provisions applicable to the approval of Service Providers/Contractors/Subprocessors are listed in Section 2 of Annex B to this DPA.

8. **Compliance With CCPA.** To the extent that the Processing of Personal Data that constitutes Personal Information is subject to the CCPA, Company shall comply with applicable obligations under the CCPA. Company shall provide the same level of privacy protection with respect to Personal Data that it receives pursuant to this DPA as required of Businesses under the CCPA. If Company determines that it can no longer meet its obligations under the CCPA, it shall notify Customer in writing (including by email).

9. **Monitoring Compliance with State Privacy Laws.** Customer shall have the right to take reasonable and appropriate steps to help to ensure that Company uses the Personal Data in a manner that is consistent with Customer's obligations under State Privacy Laws. The Parties agree that those reasonable and appropriate steps are listed in Section 5 of Annex B to this DPA, which is hereby incorporated into this Annex C by this reference.

10. **Remediating Unauthorized Use.** Customer shall have the right to take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Data, including by requiring Compamy to provide documentation that verifies that it no longer retains or uses Personal Data of Consumers that have made a valid request to delete under State Privacy Laws to Customer.

11. **Combining Personal Information.** Company shall not combine Personal Data that Company receives from, or on behalf of, Customer with Personal Data that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the Data Subject (except to perform a Business Purpose as defined under applicable State Privacy Laws).

12. **Assistance With Data Subject Requests.** Customer shall inform Company of any consumer request made pursuant to State Privacy Laws that Company must comply with and provide information necessary for Company to comply with the request.

ANNEX D TO DPA

SECURITY MEASURES

The technical and organisational measures implemented by Company pursuant to Section 4.2 of the DPA shall be as follows:

1. **Security Staffing and Background Checks.**
   - Organizational management and dedicated staff responsible for the development, implementation and maintenance of Company's information security program.
   - Employees are subject to background checks prior to employment.
   - Employees must complete management-approved security training during onboarding and revisit such training annually throughout their tenure.
2. **Audit and Risk Assessment.** Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Company's organization, monitoring and maintaining compliance with Company's policies and procedures, and reporting the condition of Company's information security and compliance to internal management.
3. **Security Controls.** Data security controls which include, at a minimum:
   - Logical segregation of data;
   - Restricted (e.g. role-based) access and monitoring; and
   - Utilization of encryption technologies for Personal Data that is transmitted over public networks (i.e. the Internet) or when transmitted wirelessly or at rest or stored on portable or removable media (i.e. laptop computers, CD/DVD, USB drives, back-up tapes).
4. **Access Controls.**
   - Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (*e.g.* use of unique IDs and passwords for all users, periodic review and revoking/changing access promptly when employment terminates or changes in job functions occur).
5. **Password Security.** Password controls designed to manage and control password strength, expiration and usage, including prohibiting users from sharing passwords and requiring that Company's passwords that are assigned to its employees:
   - Be at least eight (8) characters in length;
   - Not be stored in readable format on Company's computer systems; and
   - Newly issued passwords must be changed after first use.
6. **System Event Logging.** System audit or event logging and related monitoring procedures to proactively record user access and system activity.
7. **Physical Security.** Physical and environmental security of areas containing Personal Data managed by Company that are designed to:
   - Protect information assets from unauthorized physical access;
   - Manage, monitor and log movement of persons into and out of Company's facilities; and
   - Guard against environmental hazards such as heat, fire and water damage.
8. **Operational Procedures.** Operational procedures and controls designed to provide for configuration, monitoring and maintenance of technology and information systems,

including secure disposal of systems and media designed to render data contained therein as undecipherable or unrecoverable prior to final disposal or release from Company's possession.

9. **Change Management.** Change management procedures and tracking mechanisms designed to test, approve and monitor all material changes to Company's technology and information assets.

10. **Incident response.** Incident response management procedures designed to allow Company to investigate, respond to, mitigate and notify of events related to Company's technology and information assets.

11. **Network Security.** Network security controls that utilize firewalls and segregated access, and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.

12. **Vulnerability Management Processes.**

- Vulnerability assessment, patch management and threat protection technologies, and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code; and

- Third party vulnerability assessments are conducted periodically and vulnerabilities are remediated as appropriate in accordance with Clompany's internal risk assessment policies.

13. **Policy Review.** Company's security and privacy policies are reviewed and approved annually for Company's business operations.