ThoughtExchange® Data Processing Addendum

This Data Processing Addendum ("DPA") forms part of the ThoughtExchange Subscription Agreement, or other agreement governing the use of the Subscription Services ("Agreement") entered by and between you ("you", "your", "Customer"), and the ThoughtExchange entity identified in the Agreement ("us", "we", "ThoughtExchange"). This DPA reflects the parties' agreement with regard to the Processing of Personal Data in accordance with the requirements of Data Protection Laws and Regulations. All capitalized terms not defined herein will have the meaning set forth in the Agreement.

In the course of providing the Subscription Services to you pursuant to the Agreement, we may Process Personal Data on your behalf. We agree to comply with the following provisions with respect to any Personal Data.

1. DEFINITIONS

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

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

"Data Protection Laws and Regulations" means laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, applicable to the Processing of Personal Data under the Agreement.

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

"GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as may be amended, superseded or replaced.

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

"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.

"Sub-processor" means any Data Processor engaged by ThoughtExchange.

"Supervisory Authority" means an independent public authority established by a European Union member state pursuant to the GDPR.

2. PROCESSING OF PERSONAL DATA

2.1 Roles of the Parties. With regard to the Processing of Personal Data, you are the Data Controller and we are a Data Processor. We will engage Sub-processors pursuant to the requirements set forth in Section 5 "Sub-processors" below.

2.2 Customer Processing of Personal Data. You will, in your use of the Subscription Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, your instructions for the Processing of Personal Data will comply with Data Protection Laws and Regulations. You will have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which you acquire Personal Data.

2.3 ThoughtExchange Processing of Personal Data. We will only Process Personal Data on behalf of and in accordance with your instructions and will treat Personal Data as Confidential Information. You instruct us to Process Personal Data for the following purposes: (i) Processing in accordance with the Agreement and applicable Service Order; (ii) Processing initiated by Authorized Users in their use of the Subscription Services; (iii) Processing to comply with other reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement; (iv) rendering Personal Data fully and irrevocably anonymous and non-personal; and (v) Processing as required under any applicable laws to which we ae subject, provided that we will inform you of the legal requirement before Processing, unless prohibited under such law.

2.4 Scope and Purpose. The objective of Processing of Personal Data by ThoughtExchange is the performance of the Subscription Services pursuant to the Agreement.

2.5 Type of Personal Data. You and your Authorized Users determine the identity of Participants, and the type and

nature of any Personal Data (if any) uploaded to the Subscription Services. We have no control over the identity of the data subjects whose Personal Data is processed on your behalf and over the types of Personal Data Processed.

3. RIGHTS OF DATA SUBJECTS

3.1 Correction, Blocking and Deletion. To the extent that you, in its use of the Subscription Services, do not have the ability to correct, amend, block, transfer, or delete Personal Data as required by Data Protection Laws and Regulations, we will comply with any commercially reasonable request to facilitate such actions to the extent we are legally permitted to do so.To the extent legally permitted, you will be responsible for any costs arising from such assistance.

3.2 Data Subject Requests. We will, to the extent legally permitted, promptly notify you if we receive a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, object to the Processing, or its right not to be subject to an automated individual decision making ("Data Subject Request"). Taking into account the nature of the Processing, we will assist you by taking appropriate technical and organizational measures, insofar as possible, with fulfilling your obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent you, in your use of the Subscription Services, do not have the ability to address a Data Subject Request, we will upon your request provide commercially reasonable efforts to assist you in responding to such Data Subject Request, to the extent we are legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, you will be responsible for any costs arising from such assistance.

4. PERSONNEL

4.1 Confidentiality. We will ensure that our 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.

4.2 Data Protection Officer. We have appointed a data protection officer where such appointment is required by Data Protection Laws and Regulations. The appointed person may be reached at privacy@thoughtexchange.com.

5. SUB-PROCESSORS

5.1 Appointment of Sub-processors. You acknowledge and agree that (a) our Affiliates may be retained as Sub-processors; and (b) ThoughtExchange and our Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Subscription Services. We will enter agreements with our Sub-processors containing materially similar data protection obligations as set forth herein. You specifically authorize the engagement of those Sub-processors listed at < https://www.thoughtexchange.com/subprocessors/ > as updated from time to time.

5.2 Liability. Except as otherwise set forth in the Agreement, we will be liable for the acts and omissions of our Sub-processors to the same extent that we would be liable if performing the services of each Sub-processor directly under the terms of this DPA.

6. SECURITY

6.1 Controls for the Protection of Personal Data. We will maintain reasonable administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Content, including Personal Data. We regularly monitor compliance with these safeguards. We will not materially decrease the overall security of the Subscription Services during a subscription term.

6.2 Third-Party Certifications and Audits. We have obtained third-party certifications and audits. Upon your written request, we will make available to you or your independent third-party auditor (so long as neither is a competitor of ThoughtExchange) a copy of our then most recent third-party audits or certifications, as applicable, or any summaries thereof, that we generally makes available to our customers at the time of such request.

7. SECURITY BREACH MANAGEMENT AND NOTIFICATION We maintain security incident management policies and procedures and will, to the extent permitted by law, promptly notify you without undue delay of any actual or reasonably suspected unauthorized disclosure of Personal Data by us or our Sub-processors of which we become aware (a "Security Breach"). To the extent reasonably feasible, our breach notification to you will include the nature of the personal data breach, the name and contact of our data protection officer, the likely consequences of the personal data breach and the measures being taken to address the breach. We will cooperate with you to assist you in meeting any legally required notificationobligations. We will make reasonable efforts to identify and remediate the cause of such Security Breach. Such identification and remediation efforts will be made at our expense unless you or your Authorized Users caused the Security Breach.

8. EUROPEAN PERSONAL DATA

8.1 GDPR. We will Process Personal Data in accordance with the GDPR requirements directly applicable to our provision of the Subscription Services. Upon your request, we will provide you with reasonable cooperation and assistance needed to fulfill your obligation under the GDPR to carry out a data protection impact assessment related to your use of the Subscription Services, to the extent you do not otherwise have access to the relevant information, and to the extent such information is available to us. We will provide reasonable assistance to you in the cooperation with the Supervisory Authority to the extent required under the GDPR.

8.2 Transfer Mechanisms. To the extent we are a recipient of and process Personal Data protected by data protection and privacy laws enacted in Member States of the European Union, plus Iceland, Liechtenstein, Norway, Switzerland and the United Kingdom in a country that does not provide an adequate level of protection for Personal Data, the parties agree to the following:

8.2.1 In relation to transfers of Personal Data protected by the GDPR, you acknowledge that you are a controller; accordingly the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (the "EU SCCs") shall apply to such transfers, completed as follows:

i. Module Two (*controller to processor transfer*) of the EU SCCs shall apply;

ii. in Clause 7, the optional docking clause will apply;

iii. in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processor changes shall be as set out in Section 8.6 of this DPA;

iv. in Clause 11, the optional language will not apply;

v. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;

vi. in Clause 18(b), disputes shall be resolved before the courts of Ireland;

vii. Annex I of the EU SCCs shall be deemed completed with the information set out in Annex A to this DPA; and

viii. Annex II of the EU SCCs shall be deemed completed with the information set out in Annex B to this DPA.

8.2.2 Subject to Section 8.2.3, below, in relation to transfers of Personal Data protected by the GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018, the EU SCCs will apply to such transfers in accordance with Section 8.2.1 above with the following modifications:

i. any references in the EU SCCs to "Directive 95/46/EC" or "Regulation (EU) 2016/679" shall be interpreted as references to the UK GDPR; references to specific Articles of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK GDPR;

ii. references to "EU", "Union" and "Member State law" are all replaced with "UK"; Clause 13(a) and Part C of Annex II of the EU SCCs are not used; references to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the Information Commissioner and the courts of England and Wales;

iii. Clause 17 of the EU SCCs is replaced to state that "The Clauses are governed by the laws of England and Wales" and Clause 18 of the EU SCCs is replaced to state "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may bring legal proceeding 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".

8.2.3 To extent that and for so long as the EU SCCs as implemented in accordance with Section 8.2.1 and 8.2.2 above cannot be used to lawfully transfer Personal Data in compliance with the UK GDPR, the applicable standard data protection clauses for processors adopted pursuant to Article 46(2)© or (d) of the UK GDPR (the "UK SCCs") shall be incorporated by reference and form an integral part of this DPA and shall apply to transfers governed by the UK GDPR. For the purposes of the UK SCCs, the relevant Annexes of the UK SCCs shall be populated using the information contained in Annexes A and B (as applicable) of this DPA.

8.3 Sub-processor Obligations. We will enter into a written agreement with each Sub-processor imposing data protection obligations no less protective of Personal Data as required by this DPA (to the extent applicable, considering the nature of the services provided by the Sub-processor).

8.4 List of Subprocessors. A list of our Sub-processors, including their functions and locations, is available at < https://www.thoughtexchange.com/subprocessors/ > and may be updated by us from time to time in accordance with this DPA.

8.5 Changes to Sub-processors. When we engage a new Sub-processor, we will notify you of the engagement, which notice may be given by privacy@thoughtexchange.com. We will give such notice at least ten (10) calendar days before the new Sub-processor Processes any Personal Data, except that if we reasonably believe engaging a new Sub-processor on an expedited basis is necessary to protect the confidentiality, integrity or availability of the Personal Data or avoid material disruption to the Subscription Services, we will give such notice as soon as reasonably practicable. If, within five (5) calendar days after such notice, you notify us in writing that you object to our appointment of a new Sub-processor based on reasonable data protection concerns, the parties will discuss such concerns in good faith and whether they can be resolved. If the parties are not able to mutually agree to a resolution of such concerns, you, as your sole and exclusive remedy, may terminate the Agreement for convenience.

8.6 Audits and Certifications. Upon your request, and subject to the confidentiality obligations set forth in the Agreement, we will make available to you (or your independent, third-party auditor that is not our competitor) information regarding our compliance with the obligations set forth in this DPA in the form of the third-party certifications and audits (such as SOC 2) to the extent we make them generally available to our customers ("Audit Reports"). You agree that any audit rights granted by applicable data protection laws will be satisfied by the Audit Reports. To the extent that our provision of an Audit Report does not provide sufficient information for you to verify our compliance with this DPA or if you required to respond to a regulatory authority audit, you may contact us to request an audit of the procedures relevant to the protection of Personal Data. You will reimburse us for any time expended for any such audit. Before the commencement of any such audit, the parties will mutually agree upon the auditor, scope, timing, and duration of the audit in addition to the reimbursement rate. You will promptly notify us of information regarding any non-compliance discovered during the course of an audit.

8.7 Conflict. In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses in Attachment 1,the Standard Contractual Clauses will prevail.

9. CALIFORNIA. To the extent that Personal Data is subject to the California Consumer Protection Act ("CCPA"), we agree that we shall process Personal Data as a service provider and shall not (a) retain, use or disclose Personal Data for any purpose other than the purposes set out in the Agreement and this DPA and as permitted by the CCPA; or (b) "sell" personal information (as defined and understood within the requirements of the CCPA).

10. LIMITATION OF LIABILITY Each party's and its Affiliates' liability arising out of or related to this DPA is subject to the Limitation of Liability section of the Agreement, whether based in contract, tort or under any other theory of liability.

11. GENERAL

11.1 Conflict with Agreement. Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict.

11.2 Permitted Modifications. Notwithstanding anything else to the contrary in the Agreement, we may periodically modify this DPA as may be required to comply with Data Protection Law.

11.3 Severability. The provisions of this DPA are severable. If any phrase, clause or provision or attachment (including the Standard Contractual Clauses) is invalid or unenforceable in whole or in part, such invalidity or unenforceability shall affect only such phrase, clause or provision, and the rest of this DPA or the remainder of the Agreement, which shall remain in full force and effect.

11.4 Governing Law and Venue. This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by Data Protection Law.

ANNEX A

A. LIST OF PARTIES

Data Exporter	**Data Importer**
Name:	**Name:** Fulcrum Management Solutions Ltd. (ThoughtExchange)
Address:	**Address:** Suite E, 1990 Columbia Avenue, Rossland, BC, V0G 1Y0
Contact Person's Name, position and contact details:	**Contact Person's Name, position and contact details:** Chris Mussell VP Information Security and Privacy privacy@thoughtexchange.com
Activities relevant to the transfer: See (B) Below	**Activities relevant to the transfer: See (B) Below**
Role: Controller	**Role: Processor**

B. DESCRIPTION OF PROCESSING / TRANSFER

Categories of Data Subjects:	
The personal data transferred concerns the following categories of data subjects	Customers may submit Personal Data to the ThoughtExchange application, to the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, but is not limited to, Personal Data relating to the following data subjects: • Leader and participant contact details • Fields defined by customer in a CSV data import • Responses to demographic or survey questions asked by the customer
Purpose(s) of the transfer:	
The transfer is made for the following purposes:	Processing (a) to perform any steps necessary for the performance of the Agreement; (b) to provide the Subscription Services in accordance with the Agreement; (c) initiated by Users in their use of the Subscription Services; (d) to comply with other reasonable instructions provided by Client that are consistent with the terms of the Agreement and this DPA; and (e) to comply with any legal obligations under applicable law, including Data Protection Law.
Categories of Personal Data:	
The personal data transferred concern the following categories of data:	The types of Personal Data processed by ThoughtExchange are determined and controlled by the Customer in its sole descension and may include, but are not limited to, the following categories of Personal Data: • Contact data (name, email address, phone number) • Fields defined by customer in a CSV data import
Frequency of the transfer:	
whether the data is transferred on a one-off or continuous basis.	Continuous.
Sensitive data (if appropriate):	
The personal data transferred concern the following categories of special / sensitive Personal Data:	The types of Personal Data processed by ThoughtExchange are determined and controlled by the Customer in its sole discretion. Under the terms of the Agreement, Customers should not provide ThoughtExchange with Prohibited Data.
Duration of processing:	The duration of the data processing under this DPA is until the termination of the Agreement in accordance with its terms plus the period from the expiry of the Agreement until deletion of Personal Data in accordance with the terms of the Agreement.
Nature of processing:	Personal Data transferred will be processed in accordance with the Agreement (including this DPA) and may be subject to the following processing activities: (i) storage and other processing necessary to provide, maintain and improve the Subscription Service (as applicable); and/or (ii) disclosures in accordance with the Agreement or this DPA and/or as compelled by applicable laws.

…

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority, in accordance with Clause 13 of the EU SCCs, must be (i) the supervisory authority applicable to the data exporter in its EEA country of establishment or, (ii) where the data exporter is not

established in the EEA, the supervisory authority applicable in the EEA country where the data exporter's EU representative has been appointed pursuant to Article 27(1) of the GDPR, or (iii) where the data exporter is not obliged to appoint a representative, the supervisory authority applicable to the EEA country where the data subjects relevant to the transfer are located. With respect to Client Data regulated by the UK GDPR, the competent supervisory authority is the Information Commissioners Office (the "***ICO***").

ANNEX B
TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA
Technical and organization security measures implemented by ThoughtExchange
https://www.thoughtexchange.com/security/

SPECIFIC MEASURES

Measure	Description
Measures of encryption of personal data	ThoughtExchange has taken the following measures to encrypt personal data: • Data transmitted over public networks via TLS is encrypted with TLS 1.2 or higher • Data at rest is encrypted using AES256 or stronger Note: email should not be used for sending personal data.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	**Confidentiality** ThoughtExchange has taken the following measures to ensure Customer data is accessed only by authorized persons: • Multi Factor Authentication on all supporting systems • Privileged access is not granted to any system by default • Customer data is encrypted in transit and at rest • All ThoughtExchange employees and contractors participate in annual security and privacy training • Development, Test and Production environments are separate by design **Integrity** ThoughtExchange takes the following measures to ensure the integrity of customer data: • Customer data is encrypted in transit and at rest • Security and Development Operations Teams have tools in place for audit trails, event logging, intrusion detection and file integrity for all cloud systems **Availability and Resilience** ThoughtExchange takes the following measures to ensure data is protected from accidental destruction or loss and ensure availability: • Alerting is configured for specific performance thresholds • Intrusion Detection and File Integrity systems are monitored 24x7 • High availability clustering is used to increase availability • Routine backups are taken and stored offsite for production systems
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	Thoughtexchange has taken the following measures to ensure restoration of customer data in the event of a physical or technical incident: • ThoughtExchange maintains an Incident Response Plan that is tested and updated at least annually • Routine backups are taken and stored offsite • Systems are monitored for capacity and future resource planning
Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures to ensure the security of the processing	In addition to maintaining SOC 2 Type 2 compliance ThoughtExchange takes the following measures to review security of processing: • Web application penetration, OS and Network testing is completed internally with each software release • Third party web application penetration, OS and network testing is completed annually • ThoughtExchange also maintains a private “bug bounty” program

Measures for user identification and authorization	ThoughtExchange maintains the following measures for user identification and authorization: • ThoughtExchange maintains administrative controls under the principle of least privilege • Single Sign On and Multifactor Authentication is required for all non-public systems
Measures for ensuring physical security of locations at which personal data are processed	ThoughtExchange relies on our cloud hosting providers to maintain physical security: • ThoughtExchange reviews cloud hosting provider security at lease annually • All data stored at cloud hosting providers is encrypted by ThoughtExchange
Measures for ensuring events logging	ThoughtExchange maintains the following event logging: • User activity logs • Server logs • Audit logs
Measures for ensuring system configuration, including default configuration	ThoughtExchange has defined baseline configurations for all deployed systems and deploys new systems as code from hardened playbooks.
Measures for internal IT and IT security governance and management	ThoughtExchange has a dedicated security and compliance team and is audited annually against the SOC 2 Type 2 standard
Measures for certification/assurance of processes and products	ThoughtExchange has a dedicated security and compliance team and is audited annually against the SOC 2 Type 2 standard
Measures for ensuring data minimization	ThoughtExchange allows Customers to control the personal data collected by the ThoughtExchange application
Measures for ensuring data quality	ThoughtExchange has established processes for data subjects to exercise their data rights to amend and update their information
Measures for ensuring limited data retention	ThoughtExchange has an established process to ensure data is deleted in accordance with the terms of the Customers Agreement
Measures for ensuring accountability	ThoughtExchange has a VP Information Security and Privacy who is responsible for privacy related obligations and performs privacy impact assessments for new processing activities
Measures for allowing data portability and ensuring erasure	ThoughtExchange has established processes to comply with section 3.2 Data Subject Requests of the DPA
Technical and organizational measures to be taken by the [sub]-processor to provide assistance to the controller and, for transfers from a processor to a [sub]-processor, to the Customer.	When ThoughtExchange engages a sub-processor, ThoughtExchange enter into and agreement with data protection obligations similar to those in this Addendum. Each sub-processor agreement must ensure that ThoughtExchange is able to meet its obligations to our Customer. In addition to implementing technical and organizational measures to protect personal data, sub-processors must (a) notify ThoughtExchange in the event of a Security Incident so ThoughtExchange may notify Customers; (b) delete personal data when instructed by ThoughtExchange in accordance with Customer's instructions to ThoughtExchange; (c) not engage additional sub-processors without Thoughtexchange's authorization; d) not change the location where personal data is processed; or (e) process personal data in a manner which conflicts with Customer's instructions to ThoughtExchange.