Shared Assessments
Data Processing Addendum

1. Introduction

1.1. This Data Processing Addendum ("**Addendum**") sets out the parties' respective rights and obligations in relation to the Processing of Personal Data as part of Shared Assessments Subscription Agreement (the "**Agreement**") between Shared Assessments and the Customer (as defined in the Agreement) and is effective as of the date of the Agreement.

1.2. Each party shall comply with Data Protection Laws that govern its Processing of Personal Data in connection with the Agreement.

2. Customer's Responsibilities

2.1. The Customer shall have sole responsibility for the accuracy and quality of Personal Data provided by or on behalf of the Customer to Shared Assessments.

2.2. The Customer represents and warrants to Shared Assessments that it has established all rights (including, where relevant, providing a privacy notice and obtaining any necessary consents) under applicable law for Shared Assessments to Process Personal Data to provide the Services and comply with the Agreement and this Addendum.

2.3. The Customer shall provide to Shared Assessments only the minimum Personal Data required for Shared Assessments to fulfil its obligations under the Agreement and shall take appropriate technical and organizational measures to ensure the security of the Personal Data and to protect against the unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data, including ensuring that Personal Data is securely transferred to Shared Assessments.

2.4. The Customer represents and warrants to Shared Assessments that Processing by Shared Assessments under the Agreement: (i) does not and shall not violate applicable law or, if applicable, the Customer's obligations under other agreements or privacy notices provided to Data Subjects; and (ii) the Customer will not request Shared Assessments to use, disclose or otherwise Process Personal Data in any manner that would not be permissible under applicable law.

2.5. Where required by and in accordance with Data Protection Laws, the Customer will be responsible for, and will handle, any Data Subject Requests, and any other relevant requests or complaints in relation to the Personal Data.

2.6. The Customer shall: (i) be responsible for all communications and correspondence with Regulators in relation to the Processing of Personal Data; and (ii) keep Shared Assessments informed of such communications and correspondence to the extent permitted by law, unless in either case a Regulator requests in writing to engage directly with Shared Assessments or the parties (acting reasonably and taking into account the subject matter of the request) agree that Shared Assessments shall handle a Regulator request itself.

3. Shared Assessments' Responsibilities

3.1. Shared Assessments shall Process Personal Data only as reasonably related to the Services and within the direct business relationship between the parties and Shared Assessments shall not otherwise retain, use, disclose, combine, Sell or Share Personal Data except as permitted pursuant to Data Protection Laws.

3.2. To the extent permitted by Data Protection Laws, Shared Assessments may create or derive from Processing Personal Data aggregated or de-identified data that does not reasonably identify the Customer or any Data Subject and use, retain, or disclose such aggregated or de-identified data to third parties to improve Shared Assessments' products and services and for its other lawful business purposes, including as set out in the Agreement.

3.3. To the extent that Shared Assessments acts as a Processor on behalf of the Customer as a Controller, or as a sub-Processor on behalf of the Customer as a Processor (in which case the Customer warrants and represents on a continuous basis that it has authority from the Controller to bind Shared Assessments as a sub-Processor), as made clear in the applicable Agreement or by operation of Data Protection Laws, the subject-matter, duration, nature and purpose of the Processing by Shared Assessments and the type of Personal Data and categories of Data Subjects are specified in Attachment 1 (Data Processing Details) to this Addendum or as contemplated by the applicable Agreement and Shared Assessments shall:

3.3.1. only Process Personal Data in accordance with the Customer's documented instructions as completely and finally set out in this Addendum and each applicable Agreement or as required to comply with applicable law;

3.3.2. ensure that persons authorized to Process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

3.3.3. taking into account the state of the art, costs of implementation, the nature of Processing and the risk to the rights of Data Subjects, maintain the technical and organizational measures set out in Attachment 2 (Security Measures) for the purpose of protecting the confidentiality, integrity, availability and resilience of Shared Assessments systems which are involved in Processing Personal Data and which are designed to protect against the unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data in Shared Assessments' possession, custody or control. The Customer has assessed the level of security appropriate to the Processing in the context of its obligations under Data Protection Laws and agrees that the security measures set out in Attachment 2 (Security Measures) are appropriate for the Processing of Personal Data under the Agreement;

3.3.4. without prejudice to any subcontracting provisions in the Agreement, where required by Data Protection Laws, only engage another Processor of Personal Data subject to substantially equivalent data protection obligations as set out this Section 3.3 and Shared Assessments remaining fully liable for such other Processor's performance of such data protection obligations and the Customer generally authorizes the use of other Processors on this basis, provided that Shared Assessments shall inform the Customer of any other new Processors

reasonably in advance, thereby giving the Customer the opportunity to object to such changes;

3.3.5. transfer Personal Data out of the European Economic Area and/or the United Kingdom only subject to the Standard Contractual Clauses to which the following shall apply:

3.3.5.1. Module Two (Transfer Controller to Processor) of the Standard Contractual Clauses shall apply where Shared Assessments acts as a Processor on behalf of Customer as a Controller;

3.3.5.2. Module Three (Transfer Processor to Processor) of the Standard Contractual Clauses shall apply where Shared Assessments acts as a sub-Processor on behalf of Customer as a Processor; and

3.3.5.3. the following sections of this Addendum shall apply to the Standard Contractual Clauses, provided that these shall not operate to contradict the Standard Contractual Clauses:

(a) for the purposes of the Standard Contractual Clauses, the instructions to Shared Assessments as data importer shall be any instructions issued in accordance with Section 3.3.1 of this Addendum;

(b) Section 3.3.7 of this Addendum shall apply to any enquiries, requests or complaints from a Data Subject that Shared Assessments is obliged to deal with in accordance with the Standard Contractual Clauses;

(c) Section 3.3.4 of this Addendum shall apply in respect of any sub-processing by Shared Assessments as data importer; and

(d) Section 3.3.10 of this Addendum shall apply in respect of any obligations that Shared Assessments might have under clause 8.9 (Documentation and Compliance) of the Standard Contractual Clauses;

3.3.6. without undue delay notify the Customer if it becomes aware of a Personal Data Breach or receives a request from a Data Subject or Regulator, in each case in relation to the Personal Data that it Processes as a Processor on behalf of the Customer;

3.3.7. taking into account the nature of Shared Assessments' Processing of Personal Data and insofar as this is possible, provide reasonable cooperation to the Customer in relation to the Customer's obligations under Data Protection Law to respond to Data Subjects exercising their rights under Data Protection Law;

3.3.8. assist Customer with complying with its obligations to carry out data protection impact assessments and prior consultations of Regulators where required by Data Protection Law by providing the information set out in the Agreement, this

Addendum and the Shared Assessments privacy notice, and as referred to in Section 3.3.10;

3.3.9. at the choice of Customer, after the end of the provision of the Services relating to Processing, delete or return to Customer all Personal Data in Shared Assessments' possession or control in accordance with Shared Assessments' document retention and deletion policies, and delete existing copies in accordance with Shared Assessments' backup and disaster recovery procedures, unless applicable law or record retention requirements require otherwise; and

3.3.10. make available to the Customer all information reasonably necessary to demonstrate compliance with applicable Data Protection Laws and allow for and contribute to audits, including inspections, solely by providing the Customer with, upon reasonable request: (i) a summary of its information security and privacy policies applicable to the Services; (ii) any customer-releasable summaries of audit reports performed by a qualified third-party auditor within twelve (12) months of the Customer's request; and (iii) cooperation in responding to reasonable enquiries from the Customer relating to the results of such summary information.

3.4. To the extent that any U.S. State Privacy Law applies to Shared Assessments' Processing of Personal Data under the Agreement, including the California Consumer Privacy Act, as amended by the California Privacy Rights Act (Cal. Civ. Code § 1798.100 et seq.) (collectively, "CCPA"), the following obligations shall apply:

3.4.1. Shared Assessments shall promptly notify the Customer if it determines that it can no longer meet its obligations under applicable U.S. State Privacy Laws with respect to the Personal Data it Processes on behalf of the Customer.

3.4.2. Upon receipt of such notification under Section 3.4.3, or if the Customer otherwise has a reasonable and good-faith belief that Shared Assessments is Processing Personal Data in a manner not authorized by this Addendum or applicable U.S. State Privacy Laws, the Customer shall have the right to take reasonable and appropriate steps to stop and remediate such unauthorized Processing.

4. **General**

4.1. **Costs.** In the event that the Customer requests cooperation or assistance from Shared Assessments which exceeds that which is required in order to comply with Data Protection Laws, Shared Assessments reserves the rights to charge for such cooperation or assistance.

4.2. **Termination.** Notwithstanding anything in the Agreement to the contrary, this Addendum will terminate when Shared Assessments ceases to Process Personal Data, unless otherwise agreed in writing between the parties.

4.3. **Liability.** The parties agree that all liabilities between them relating to the Processing of Personal Data are governed by the limitations and exclusions of liability and other terms of the Agreement.

4.4. **Data Processing Details.** Attachment 1 is provided for information purposes and compliance with Data Protection Laws and Attachment 1 shall not impose any obligations or create any rights for either party.

4.5. **Exclusion of third party rights.** All third-party rights are excluded except where Shared Assessments determines that it must grant such rights pursuant to Data Protection Laws and the Standard Contractual Clauses and only to the extent required by Data Protection Laws and the Standard Contractual Clauses. All other third-party rights are excluded.

4.6. **Governing Law.** This Addendum shall be governed by the laws of the jurisdiction specified in the Agreement.

5. **Definitions**

5.1. "**Controller**" means the party which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

5.2. "**Data Protection Laws**" means all applicable laws and regulations relating to the Processing of Personal Data pursuant to the Agreement.

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

5.4. "**Data Subject Request**" means a Data Subject's request to exercise their rights under Data Protection Laws.

5.5. "**Personal Data**" means information that identifies or could reasonably be used to identify an individual, including "personal data," "personal information," "personally identifiable information," or an equivalent term, as defined by, and subject to protection under, Data Protection Laws, to the extent such information is provided by or on behalf of the Customer to Shared Assessments pursuant to the Agreement.

5.6. "**Personal Data Breach**" means: (i) any security incident involving Personal Data which is notifiable to the other party, Privacy Regulators or Data Subjects under Data Protection Laws; or (ii) the actual unauthorized access to, acquisition, or use of unencrypted Personal Data in Shared Assessments' custody or control that materially compromises the security, confidentiality or integrity of such Personal Data and has the potential to cause identity theft or financial harm to individuals whose Personal Data was aEected.

5.7. "**Processing**", "**Processed**" or "**Process**" means any operation or set of operations which is performed by either party as part of, or in connection with, the Services upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

5.8. "**Processor**" means, to the extent applicable within scope of Data Protection Laws, a natural or legal person, public authority, agency or other body which Processes personal data on behalf of the Controller.

5.9. "**Regulator**" means any governmental authority or regulator with authority under Data Protection Laws over the Processing of Personal Data.

5.10. "**Sell**" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration.

5.11. "**Share**" means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for cross-context behavioral advertising.

5.12. "**Services**" means all work performed under the Agreement and all activities relating to such work and the Agreement, including without limitation to: (a) carry out the proper administration, assessment and improvement of the business of Shared Assessments and its aEiliates; (b) administer and manage the customer relationship and compliance with the Agreement; (c) establish, exercise or defend legal claims in respect of the Agreement; and (d) comply with any applicable legal or self-regulatory obligations.

5.13. "**Standard Contractual Clauses**" means: the agreement in the form in the C(2021) 3972 final Annex to the Commission Implementing Decision 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, which is hereby incorporated into and subject to the terms of this Addendum and completed as follows: (a) Clause 17 is deemed completed with Option 2 and the law of the EU Member State in which the data exporter is established; (b) Clause 18 is deemed completed with the law of the EU Member State in which the data exporter is established; (c) Annex I is deemed to be populated with the names and contact information of the Customer and Shared Assessments as set out in the Agreement and this Addendum; (d) the categories of data subjects and Personal Data and the nature and purposes of the processing in Annex I is deemed to be populated as set out in Attachment 1 to this Addendum; (e) the sections of Annex I requiring details of the frequency of the transfer is deemed populated with, 'As needed to comply with the terms of the Agreement and the Addendum'; (f) the period for which the Personal Data will be retained in Annex 1 is deemed populated with 'Until such personal data transferred pursuant to these Clauses is returned or destroyed in accordance with and subject to the terms of the Agreement and the Addendum'; (g) transfers to sub-processors in Annex I is deemed populated with: "Shared Assessments may engage sub-processors to process personal data transferred pursuant to these Clauses on behalf of the Customer in accordance with Option 2 of Clause 9(a), with the time period being specified as 30 days, as described in the Agreement and the Addendum"; (h) the competent supervisory authority in Annex I is deemed populated with that of where the relevant data exporter is established; (i) Annex II is deemed to be prepopulated with the technical and organizational measures described in Attachment 2 to this Addendum; and (j) to the extent required in order to comply with UK Data Protection Laws: Addendum B.1.0 (the Mandatory Clauses of the Approved Addendum) approved in accordance with s119A of the Data Protection Act 2018 on 2 February 2022 (the "**IDTA-B**"), as it is revised under section 18 of the IDTA-B shall apply, with neither party having the right to end the IDTA-B pursuant to section 19 of the IDTA-B.

5.14. "**U.S. State Privacy Laws**" means any applicable U.S. state law or regulation governing the Processing, privacy, or protection of Personal Data, including the California Consumer Privacy Act, as amended by the California Privacy Rights Act (Cal. Civ. Code § 1798.100 et seq.), the Virginia Consumer Data Protection Act (Va. Code § 59.1-575 et seq.), the Colorado Privacy Act (Colo. Rev. Stat. § 6-1-1301 et seq.), the Connecticut Data Privacy Act (Conn. Gen. Stat. § 42-515 et seq.), and any other substantially similar U.S. state privacy or data protection law, in each case as amended or replaced from time to time.

5.15. "**UK Data Protection Laws**" means: (a) the Data Protection Act 2018; and (b) The United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, as modified by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019; each as amended or replaced from time to time.

Attachment 1 – Data Processing Details

Data subjects

The Personal Data Processed may concern the following categories of Data Subjects:

- Personnel of Customer and its aEiliates
- Any other Data Subjects whose Personal Data is uploaded by the Customer to the Platform

Categories of data

The Personal Data Processed concern the following categories of data:

- Login details (user name, user business email address)
- Any Personal Data uploaded by the Customer to the Platform

Special categories of data (if appropriate)

The Personal Data Processed may concern the following special categories of data:

- None anticipated

Processing operations

Collection, storage, analysis and disclosure of Personal Data that Shared Assessments receives from (or on behalf of) the Customer in accordance with the Agreement.

Purposes of the transfer(s)

For the purpose of complying with the Agreement and the Addendum.

Attachment 2 – Security Measures

1. Access Control

Shared Assessments implements and maintains technical and organizational measures designed to limit access to personal data and control access to it, and to protect such data against accidental destruction or loss. Access to information and information systems is controlled and managed on the basis of a demonstrated business need.

IT systems are monitored to prevent and monitor unauthorized access (for example, ID/password security). Organizational measures for user identification and authentication are implemented, as appropriate. Access controls to data are implemented, as appropriate (for example, requirements-driven definition of access rights, and monitoring and logging of access to relevant data sets).

Shared Assessments has policies and processes to require that access to personal data is restricted to only those individuals who require such access to perform their job function.

2. Physical and Environmental Security

Appropriate physical and environmental controls are implemented to ensure Shared Assessments premises, work areas and information assets are adequately protected. Shared Assessments uses industry standards to ensure that data centres are compliant with international requirements, as appropriate (for example, ISO 27001, SOC1, SOC2, PCI).

Access to facilities where information systems that process personal data are located is restricted to identified authorized individuals. Controls are implemented to control access to premises and facilities (in particular, to check authorization, security guards, CCTV, physical access restrictions).

Certain Shared Assessments applications and or data are hosted within infrastructure cloud providers or software-as-a-service (SaaS) applications that Shared Assessments utilizes for certain business functions. These providers are expected to maintain physical security controls that are equivalent to the Shared Assessments' standard physical security controls.

3. System and Network Security

Shared Assessments regularly monitors logs to detect potential cybersecurity events. Shared Assessments uses a variety of tools to monitor for unauthorized activity, anomalous behavior and indicators of compromise that require investigation. Notifications are investigated according to Shared Assessments' incident response processes to mitigate and remediate malicious activity. Monitoring is carried out by the Shared Assessments cybersecurity team of analysts with assistance from the firm's managed security services (third-party) provider.

Technical and organizational measures are implemented designed to secure data processing activities including, as appropriate, with respect to (a) data transmission and intrusion detection and monitoring; (b) end-point security (including patch management); and (c) threat and vulnerability management (including vulnerability scanning, penetration testing, threat intelligence).

4. Asset Control

Information assets are identified and an asset register is owned and maintained by Shared Assessments. Assets are protected by appropriate security controls and procedures.

5. Authentication

Shared Assessments uses industry standard practices to identify and authenticate users who attempt to access its network or information systems. Where authentication mechanisms are based on passwords, Shared Assessments requires that the passwords are renewed periodically and that they are suEiciently complex (for example, as appropriate, certain applications may utilize Single Sign On (SSO), and administrator passwords may have additional length requirements).

6. Logical Access Controls

Shared Assessments implements logical access controls to prevent unauthorized access to Shared Assessments' systems and implements safeguards to ensure authorized personnel are granted access levels appropriate to their function.

Shared Assessments: (a) maintains the ability to audit trails of personnel's access to Shared Assessments' systems; and (b) implements controls to prevent terminated or departing personnel from accessing personal data and Shared Assessments systems, including through requiring confidentiality confirmations from departing personnel upon their departure.

7. Passwords

Shared Assessments applies user authentication measures, such as strong password requirements, multi-factor authentication, and blocking access after a certain number of password errors.

8. Remote Access

Shared Assessments controls remote access to its systems from untrusted external networks using industry practice authentication mechanisms, such as two-factor authentication and using virtual private network (VPN) technology, where appropriate.

9. Privileged Accounts

Shared Assessments implements controls designed to limit the use of accounts with privileged or elevated access to Shared Assessments' systems, including those with administration-level access, to prevent misuse or unauthorized access, with appropriate processes to monitor potential misuse.

10. Malware and Hacking Protection

Shared Assessments implements technical controls designed to protect its systems from various forms of malware, including computer viruses, trojans and unauthorized third-party scripts. Software aimed at preventing the vulnerability of Shared Assessments systems and fixing bugs in relation to the same is installed and periodically updated.

11. Operational Procedures and Accountabilities

Operational procedures are documented and implemented for activities involving data processing. These procedures include:

- change management procedures;
- segregation of duties and responsibilities;
- event and incident management procedures;
- access controls and audit logging;
- software licensing; and
- vulnerability management.

12. Shared Assessments and third party agreements

Agreements and procedures are established for the exchange of any information with external parties. Data processing carried out by a data processor on behalf of Shared Assessments is to be carried out according to Shared Assessments' instructions and appropriate controls. Shared Assessments agreements are reviewed and, where appropriate, updated to ensure that Shared Assessments and third parties agree to: (a) process personal data in accordance with appropriate security, confidentiality and privacy contract terms; and (b) have in place appropriate technical and organizational measures.

13. Incident Management

Data protection, cyber security and information security incidents must be reported via the appropriate management channels as quickly and eEectively as possible to minimize the possible impact. Shared Assessments implements appropriate processes, procedures and incident response plans to assist in responding to these incidents eEectively.

14. Business Continuity Management

Shared Assessments has in place business continuity management processes and a business continuity plan ("**BCP**") to identify risks to Shared Assessments' infrastructure and systems and reduce the eEect of possible disruptions caused by disasters, man-made events and/or control failure events. The BCP is reviewed as appropriate, together with senior managers of Shared Assessments' business and support units.