INFORMATION SECURITY ADDENDUM

Last revised November 21, 2022

This Information Security Addendum ("**Addendum**") sets forth the Parties' mutual understanding relating to the privacy and security of Client Confidential Information and Client Systems.

1. **Definitions**. All terms used in this Addendum shall have the meaning specified in the Agreement unless otherwise defined herein. For the purposes of this Addendum, the following terms are defined as follows:

a. **Client Confidential Information**: All (i) information received by Phrasee from Client or a Client Affiliate, or collected or generated directly by Phrasee on Client's behalf in connection with the Services, that should reasonably be considered confidential under the circumstances, notwithstanding whether it was identified as such at the time of disclosure; (ii) all information identified as confidential to which Phrasee has access in connection with the subject matter of the Agreement, whether before or after the Effective Date of the Agreement; and (iii) the Agreement. Client Confidential Information shall include, without limitation, (A) all trade secrets (as defined under applicable law), (B) existing or contemplated products, services, designs, technology, processes, technical data, engineering, techniques, methodologies and concepts and any information related thereto, (C) information relating to business plans, sales or marketing methods and customer lists or requirements, and (D) information identifying, relating to, describing, capable of being associated with or that could be linked, directly or indirectly, with particular persons or households, including but not limited to information derived from such information that is used to create inferences regarding or profiles of such persons or households.

b. **Client System**: Any physical or technical system owned, leased, licensed or operated by Client or its Affiliates, whether on premises or hosted by a third-party, which processes Client Confidential Information and is accessed by Phrasee in the course of performing the Services.

c. **Services**: Services provided by Phrasee to Client in accordance with this Agreement and any applicable Statement of Work.

d. **Data Incident**: A breach of Phrasee's Information Security Program leading to the accidental, unlawful or unauthorized destruction, loss, alteration, disclosure of, or access to, Client Confidential Information.

2. **Compliance with Laws**.

a. During the term of the Agreement, Phrasee will comply, at its own cost and expense, with current and new laws, regulations, governmental requirements, and industry standards relating to its processing of Client Confidential Information (collectively, "Laws").

b. If Client reasonably believes that Phrasee is in non-compliance with any Laws, it shall notify Phrasee in writing of such belief. If Phrasee agrees it is in non-compliance and continues to be in non-compliance 30 days after such written notification, or Phrasee is unable to comply with any new Law, Client may, in its sole discretion, terminate the Agreement upon written notice to

Phrasee. Should a disagreement arise as to the interpretation of or Phrasee's compliance with any requirement of the Laws, the Parties shall follow the Dispute Resolution procedure as described in Section 17 of the Master Subscription Agreement.

3.   **Information Security Program.** Phrasee agrees to maintain, in writing, an information security and privacy program consistent with this Addendum and applicable Laws ("**Information Security Program**"). The Information Security Program shall include appropriate physical, technical and administrative safeguards, including any safeguards and controls sufficient to protect Client Systems and Client Confidential Information from unauthorized or unlawful destruction, loss, alteration, disclosure or access.

4.   **Security Certification**. If Phrasee maintains a certification or third-party assessment of compliance with the security standards identified in Section 3 of this Addendum provided by a qualified third party reasonably acceptable to Client, such certifications shall be provided to Client upon request.

5.   **Information Security Contact**. Phrasee's primary Information Security Contact is Matt Simmonds, Chief Product and Technology Officer, +44 (0) 7818 430 226, matt.simmonds@phrasee.co. Client's primary Information Security Contact shall be provided to Phrasee in conjunction with the most recent Service Order. Each Party agrees to promptly notify the other party of any changes to this information.

6.   **Restriction of Use of Client Confidential Information**. Except for the provision in Section 11(f) of the Master Subscription Agreement, Phrasee shall not: (i) collect, retain, use, access, rent, sell, disclose, reconfigure, de-identify, re-identify or aggregate Client Confidential Information for any purpose other than to provide the Services as set forth in this Agreement; (ii) retain, use or disclose Client Information outside of the direct business relationship between Client and Phrasee; or (iii) use Client Confidential Information to create any derivative work or product for the benefit of Phrasee or any other party without Client's express, written authorization. Any unauthorized use of Client Confidential Information shall constitute a material breach of the Agreement and, as a result, Client may, in its sole discretion, immediately suspend or terminate Phrasee's access to Client Confidential Information and Client Systems.

7.   **Audit**.

a.   Phrasee shall monitor and, at regular intervals consistent with industry best practices, test and evaluate the effectiveness of its Information Security Program and Phrasee's compliance with the terms of this Addendum. Phrasee shall evaluate and promptly adjust its practices with regards to compliance with this Addendum, including its Information Security Program, in light of the results of the testing and monitoring, any material changes to its operations or business arrangements, or any other facts or circumstances that Phrasee knows or reasonably should know may have a material impact on the use or security of Client Confidential Information and Client Systems or Phrasee's compliance with the terms of the Agreement.

b.   Phrasee shall itself regularly (at least once per year) carry out suitable tests (including vulnerability and penetration assessments) and notify Client of any findings likely to adversely impact Client Confidential Information, as well as its efforts to rectify any such issues.

Notwithstanding the above, in the event of a significant security incident by Phrasee, Client may (at its own cost) perform an audit to validate Phrasee's Information Security Program and post-incident remediation, to ensure that it remains at a level where Client can continue to conduct business under this Agreement.

c.   The above audit covers inspection of written and video Information Security Program documentation, summarised results of independent third party penetration and vulnerability tests, and limited interviews with agreed staff members. The above audit does not confer rights of access or inspection to Phrasee's infrastructure, administration areas, configuration, or other on-premises or cloud-based assets.

8.   **Breach Notification and Investigation**.

a.   Phrasee shall notify Client's Information Security Contact (as listed in Section 5 of this Appendix D) within twenty-four (24) hours of Phrasee's first detection of any identified Data Incident, followed within forty-eight (48) hours of Phrasee's first detection of the Data Incident by a written notice directed to Client's Information Security Officer. The written notice shall summarize, in reasonable detail, the nature and scope of the Data Incident (including a description of all impacted Client Confidential Information and Client Systems) and the corrective action already taken or planned by Phrasee. The notice shall be timely supplemented to the level of detail reasonably requested by Client, inclusive of relevant investigative or forensic reports.

b.   Phrasee shall promptly, at its own cost and expense, take all reasonable and necessary actions to end the Data Incident, mitigate its impact and prevent reoccurrence. Phrasee shall cooperate with Client in the investigation of the Data Incident and shall promptly respond to Client's reasonable inquiries about the Data Incident. In the event of a Data Incident, Client may, in its sole discretion, immediately suspend or terminate Phrasee's access to Client Confidential Information and Client Systems.

c.   Phrasee will not inform any third party of Client's involvement in a Data Incident (i.e. the involvement of Client Confidential Information in any breach of Phrasee's Information Security Program) without first obtaining Client's prior written consent, unless and to the extent that Phrasee is otherwise required to provide notice by laws or regulations. The Parties shall collaborate on whether to provide notice of Client's involvement in the Data Incident to any person, governmental entity, the media, or other party and the content of any such notice. Client will make the final determination as to whether notice of its involvement in a Data Incident will be provided and to whom, the content of the notice, and whether it will be the signatory to the notice. As permitted by applicable laws and regulations, Phrasee shall promptly notify Client of any investigations of its information use, privacy or information security practices or a Data Incident by a governmental, regulatory or self-regulatory body. The foregoing shall not prevent Phrasee from notifying its other clients of a data incident which has possibly impacted their confidential information, without specific reference to the involvement of Client Confidential Information. For the avoidance of doubt, Phrasee shall provide notice of a Data Incident whenever, and to whomever, it is required to do so by applicable laws or regulations.

9.   **Data Subject Rights**. To the extent that Laws require Client to comply with requests from individuals to access, delete, modify, or restrict the processing of their Personal Information, Phrasee agrees to promptly notify Client of any such requests directed to Phrasee and, no more than thirty (30) days from Phrasee's receipt of Client's written instruction, provide any assistance that Client reasonably deems necessary to fulfill such requests with regards to Services provided under the Agreement. Phrasee shall certify, in writing, its compliance with such instructions. If a consumer or other data subject exercises a legal right to opt out of the supply of their Personal Information by Client to Phrasee, Client shall not be required to provide such Personal Information to Phrasee, notwithstanding any other provision of the Agreement. To the extent Phrasee directly interacts with Client customers, employees, contractors, service providers, or other individuals while acting on behalf of Client, Phrasee agrees to provide Client with any assistance Client reasonably deems necessary to fulfill applicable legal obligations to provide such individuals with notice of data processing activities.

10.   **Subcontractors**. Phrasee shall confirm that any and all Primary Suppliers, contractors or other agents of Phrasee engaged to perform the Services comply with all applicable terms of this Addendum and relevant Laws. Phrasee shall make commercially reasonable efforts to monitor and enforce such contractual requirements and shall be responsible to Client for all acts or omissions of its subcontractors and agents with respect to their access to and use of Client Confidential Information and Systems.

11.   **Cross-border Transfers**. Phrasee shall cooperate with Client in complying with all Laws regulating the cross-border transfer of Client Confidential Information, and the Parties shall negotiate, in good faith, such additional agreements, terms and conditions as may be required by such Laws to effect such transfers. Additional information on the processing of Client Confidential Information can be found in Phrasee's Data Processing Addendum located at http://www.phrasee.co/legal/DPA .

12.   **Indemnification**. No limitation of liability provisions, if any, in the Agreement (or any other agreement between the Parties) shall apply to any breach of this Addendum by Phrasee. Notwithstanding anything in the Agreement to the contrary, Phrasee shall indemnify, hold harmless and defend Client (including its affiliates) from all suits, claims, demands, proceedings and other actions brought by a third party, and pay all expenses and costs (including but not limited to, assessments, fines, losses, penalties, settlements, costs of investigating and responding to any Data Incident, costs of notifying and providing affected individuals with at least one year of credit monitoring and fraud prevention services), arising out of or related to Phrasee's misuse of Client Confidential Information, any Data Incident or any breach by Phrasee of this Addendum.

13.   **Information Security-Related Termination Rights**. In addition to any other termination rights under the Agreement, Client shall have the right to terminate the Agreement immediately if Phrasee materially breaches any provision of this Addendum; provided however that Client first notifies Phrasee in writing of any alleged breach and provides Phrasee a reasonable opportunity to promptly remediate such breach where capable of remedy.

14.   **Statement of Compliance**. Phrasee shall provide Client with prompt written notice if at any time it learns that it is not in full compliance with the requirements of this Addendum.

Phrasee shall certify compliance with this Addendum from time to time, or as may be reasonably requested by Client.

15.   **<u>Survival; Severability</u>**. This Addendum shall survive termination of the Agreement. The invalidity or unenforceability of a portion of this Addendum shall not affect the validity or enforceability of the remainder hereof.