UNMIND: DATA PROCESSING ADDENDUM

THIS DATA PROCESSING ADDENDUM ("DPA") is entered into as of the Addendum Effective Date by and between: (1) UNMIND LIMITED, a company incorporated and registered in England and Wales with company number 10310694 with its registered office at 180 Borough High Street, London, SE1 1LB ("Unmind"); and (2) the company using the Unmind Services and signing or agreeing to this DPA ("Client"), together the “Parties” and each a “Party".

HOW AND WHEN THIS DPA APPLIES

- With effect on and from the Addendum Effective Date, this DPA is incorporated into and forms a binding and effective part of the Agreement upon its execution by the Parties.
- This DPA applies only if and to the extent Applicable Data Protection Laws govern Unmind’s Processing of Client Personal Data in performance of the Services.
- This DPA does not apply to Personal Data provided by Data Subjects directly to Unmind in connection with their use of the Services after account creation and/or during their interaction with the Unmind platform. Any such processing will be subject to Unmind’s privacy policy (available at https://unmind.com/privacy-policy?locale=en).

1. INTERPRETATION

1.1 In this DPA, the following terms shall have the meanings set out in this Section 1, unless expressly stated otherwise:

(a) “Addendum Effective Date” means (i) the date on which Client signs or agrees to this DPA or (ii) the effective date of the Agreement, whichever is earlier.

(b) “Agreement” means the agreement, statement of work or other contract entered into by and between the Parties pursuant to which Unmind provides the Services to Client and which incorporates this DPA.

(c) “Applicable Data Protection Laws” means the privacy, data protection and data security laws and regulations of any jurisdiction applicable to the Processing of Client Personal Data by Unmind under the Agreement, including, without limitation, the GDPR, the CCPA, CDPA, PIPEDA, the LGPD, and/or the Australian Privacy Act (in each case, as and where applicable).

(d) “CCPA” means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (“CPRA”), and any binding regulations promulgated thereunder.

(e) “CDPA” means the Virginia Consumer Data Protection Act.

(f) “Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

(g) “Client Personal Data” means any Personal Data Processed by Unmind or its Sub-Processors on behalf of Client to perform the Services under the Agreement, but specifically excludes any Personal Data provided by Data Subjects directly to Unmind in connection with their use of the Services.

(h) “Data Subject Request” means the exercise by a Data Subject of its rights in accordance with Applicable Data Protection Laws in respect of Client Personal Data and the Processing covered by this DPA.
“Data Subject” means an identified or identifiable natural person to whom Client Personal Data relates.

“EEA” means the European Economic Area.

“GDPR” means, as and where applicable to the Processing concerned: (i) the General Data Protection Regulation (Regulation (EU) 2016/679) (“EU GDPR”); and/or (ii) the EU GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018 (as amended, including by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019) (“UK GDPR”), including, in each case (i) and (ii) any applicable national implementing or supplementary legislation (e.g., the UK Data Protection Act 2018), and any successor, amendment or re-enactment, to or of the foregoing. References to “Articles” and “Chapters” of, and other relevant defined terms in, the GDPR shall be construed accordingly.

“Personal Data” means “personal data,” “personal information,” “personally identifiable information” or similar term defined in Applicable Data Protection Laws.

“Personal Data Breach” means a breach of Unmind’s security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Client Personal Data covered by this DPA in Unmind’s possession, custody or control. For clarity, Personal Data Breach does not include unsuccessful attempts or activities that do not compromise the security of Client Personal Data (such as unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems).

“Personnel” means an organisation’s employees, agents, consultants and/or contractors.

“Process” and inflections thereof means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“Processor” means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

“Restricted Transfer” means the disclosure, grant of access or other transfer of Client Personal Data to any person located in: (i) in the context of the EU GDPR, any country or territory outside the EEA which does not benefit from an adequacy decision from the European Commission (an “EEA Restricted Transfer”); and (ii) in the context of the UK GDPR, any country or territory outside the UK which does not benefit from an adequacy decision from the UK Government (a “UK Restricted Transfer”), which would be prohibited without a legal basis under Chapter V of the GDPR.

“SCCs” means the standard contractual clauses approved by the European Commission pursuant to implementing Decision EU 2021/914.

“Services” means those services and activities to be supplied to or carried out by or on behalf of Unmind for Client pursuant to the Agreement.

“Sub-Processor” means any third-party appointed by or on behalf of Unmind to Process Client Personal Data.

“Supervisory Authority”: (i) in the context of the EEA and the EU GDPR, shall have the meaning given to that term in the EU GDPR; and (ii) in the context of the UK and the UK GDPR, means the UK Information Commissioner’s Office.
“UK Transfer Addendum” means the template Addendum B.1.0 issued by the UK Information Commissioner’s Office (ICO) and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of the Mandatory Clauses included in Part 2 thereof (the “Mandatory Clauses”).

1.2 Unless otherwise defined in this DPA, all capitalised terms in this DPA shall have the meaning given to them in the Agreement.

2. SCOPE OF THIS DATA PROCESSING ADDENDUM

2.1 The front-end of this DPA applies generally to Unmind’s Processing of Client Personal Data in performance of the Services as a Processor, “service provider” or similar role defined under Applicable Data Protection Laws.

2.2 Annex 3 (California and Virginia Annex) to this DPA applies only if and to the extent Unmind’s Processing of Client Personal Data under the Agreement is subject to the CCPA or CDPA with respect to which Client is a “business” (as defined in the CCPA) or a “controller” (as defined in the CDPA).

3. PROCESSING OF CLIENT PERSONAL DATA

3.1 In respect of Client Personal Data, the Parties acknowledge that:

(a) Unmind acts as a Processor; and

(b) Client acts as the Controller.

3.2 Unmind shall:

(a) comply with all Applicable Data Protection Laws in Processing Client Personal Data; and

(b) not Process Client Personal Data other than:

(i) on Client’s instructions (subject always to Section 3.9); and

(ii) as otherwise required by applicable laws.

3.3 To the extent permitted by applicable laws, Unmind shall inform Client of:

(a) any Processing to be carried out under Section 3.2(b)(ii); and

(b) the relevant legal requirements that require it to carry out such Processing, before the relevant Processing of that Client Personal Data takes place.

3.4 Annex 1 (Details of Processing) sets out certain information regarding Unmind’s Processing of Client Personal Data as required by Article 28(3) of the GDPR.

3.5 Client may amend Annex 1 (Details of Processing) on written notice to Unmind from time to time as Client reasonably considers necessary to meet any applicable requirements of Applicable Data Protection Laws.

3.6 Nothing in Annex 1 (Details of Processing) (including as amended pursuant to Section 3.6) confers any right or imposes any obligation on any Party to this DPA.

3.7 Where Unmind receives an instruction from Client that, in its reasonable opinion, infringes Applicable Data Protection Laws, Unmind shall inform Client.
3.8 Client acknowledges and agrees that any instructions issued by Client with regards to the Processing of Client Personal Data by or on behalf of Unmind pursuant to or in connection with the Agreement:

(a) shall be strictly required for the sole purpose of ensuring compliance with the Applicable Data Protection Laws; and

(b) shall not relate to the scope of, or otherwise materially change, the Services to be provided by Unmind under the Agreement.

3.9 Notwithstanding anything to the contrary herein, Unmind may terminate the Agreement in its entirety upon written notice to Client with immediate effect if Unmind considers (in its reasonable discretion) that:

(a) it is unable to adhere to, perform or implement any Processing instructions issued by Client due to the technical limitations of its systems, equipment and/or facilities; and/or

(b) to adhere to, perform or implement any such Processing instructions would require disproportionate effort (whether in terms of time, cost, available technology, manpower or otherwise).

3.10 Client represents and warrants on an ongoing basis, and further shall ensure:

(a) that there is, and will be throughout the term of the Agreement, a valid legal basis and right for the Processing by Unmind of Client Personal Data in accordance with this DPA and the Agreement (including any and all instructions issued by Client from time to time in respect of such Processing) for the purposes of all Applicable Data Protection Laws; and

(b) that all Data Subjects have: (i) been presented with all required notices and statements (including as required by Article 12-14 of the GDPR (where applicable)); and (ii) provided all required consents, in each case (i) and (ii) as required under the Applicable Data Protection Laws and relating to the Processing by Unmind of Client Personal Data in accordance with this DPA and the Agreement.

3.11 Client further represents and warrants on an ongoing basis, and further shall ensure, that Client Personal Data does not and will not contain any social security numbers or other government-issued identification numbers, protected health information subject to the Health Insurance Portability and Accountability Act (HIPAA) or other information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; health insurance information; biometric information; passwords for online accounts; credentials to any financial accounts; tax return data; any payment card information subject to the Payment Card Industry Data Security Standard; Personal Data of children under 13 years of age; or any other information that falls within any ‘special categories of data’ (as that term is defined in Applicable Data Protection Laws).

3.12 Client hereby instructs Unmind to Process Client Personal Data as necessary to: (a) provide the Services to Client under and in accordance with the Agreement; and (b) create and analyse aggregated statistics on the use of the Services by Data Subjects and report on these to Client. This DPA is a complete expression of such instructions, and Client’s additional instructions will be binding on Unmind only pursuant to any written amendment to this DPA signed by both Parties.

4. UNMIND PERSONNEL

Unmind shall take commercially reasonable steps to ascertain the reliability of any Unmind Personnel who Process Client Personal Data, and shall enter into written confidentiality agreements with all Unmind Personnel who Process Client Personal Data that are not already subject to professional or statutory obligations of confidentiality.
5. **SECURITY**

5.1 Unmind shall implement and maintain those technical and organisational measures in relation to Client Personal Data, which are designed to protect Client Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access, as are described in Annex 4 (Security Measures) (the “Security Measures”).

5.2 Client acknowledges and agrees that it has reviewed the Security Measures, and that it has satisfied itself that the Security Measures are sufficient for its purposes.

5.3 Unmind may update the Security Measures from time to time, provided the updated measures do not materially decrease the overall protection of Client Personal Data.

6. **DATA SUBJECT RIGHTS**

6.1 Client acknowledges and agrees that Unmind will need to collect additional Personal Data from Data Subjects in order to grant them access to Unmind’s platform, and that in doing so, Unmind will act as the sole Controller of such additional Personal Data. Client further acknowledges and agrees that any Data Subject Request submitted to Unmind may relate to both Client Personal Data and Personal Data in respect of which Unmind is the sole Controller.

6.2 The Parties therefore agree that Unmind shall be solely responsible for receiving, addressing and responding to Data Subject Requests.

7. **PERSONAL DATA BREACH**

7.1 Unmind shall notify Client without undue delay upon Unmind’s discovering a Personal Data Breach affecting Client Personal Data. Unmind shall provide Client with information (insofar as such information is within Unmind’s possession and knowledge and does not otherwise compromise the security of any Personal Data Processed by Unmind) to allow Client to meet its obligations under the Applicable Data Protection Laws to report the Personal Data Breach. Unmind’s notification of, or response to, a Personal Data Breach shall not be construed as Unmind’s acknowledgement of any fault or liability with respect to the Personal Data Breach.

7.2 Unmind shall reasonably co-operate with Client and take such commercially reasonable steps as may be directed by Client to assist in the investigation of any such Personal Data Breach.

8. **SUB-PROCESSING**

8.1 Client generally authorises Unmind to appoint Sub-Processors in accordance with this Section 8. Unmind may continue to use those Sub-Processors already engaged by Unmind as at the date of this DPA (as those Sub-Processors are shown, together with their respective functions and locations, in Annex 5 (Authorised Sub-Processors)).

8.2 Unmind shall give Client prior written notice of the appointment of any new proposed Sub-Processor, including reasonable details of the Processing to be undertaken by the Sub-Processor. If, within seven (7) days of receipt of that notice, Client notifies Unmind in writing of any objections (on reasonable grounds) to the proposed appointment:

(a) Unmind shall use reasonable efforts to make available a commercially reasonable change in the provision of the Services, which avoids the use of that proposed Sub-Processor; and

(b) where: (i) such a change cannot be made within fourteen (14) days from Unmind’s receipt of Client’s notice; (ii) no commercially reasonable change is available; and/or (iii) Client declines to bear the cost of the proposed change, then either Party may by written notice to the other Party with immediate effect terminate the Agreement, either in whole or to the extent that it relates to the Services which require the use of the proposed Sub-Processor, as its sole and exclusive remedy.
8.3 If Client does not object to Unmind’s appointment of a Sub-Processor during the objection period referred to in Section 8.2, Client shall be deemed to have approved the engagement and ongoing use of that Sub-Processor.

8.4 With respect to each Sub-Processor, Unmind shall maintain a written contract between Unmind and the Sub-Processor that includes terms which offer at least an equivalent level of protection for Client Personal Data as those set out in this DPA. Unmind shall remain liable for any breach of this DPA caused by a Sub-Processor.

9. **AUDIT RIGHTS; ASSISTANCE**

9.1 Taking into account the nature of the Processing of Client Personal Data by Unmind and the information available to Unmind, Unmind shall provide such information and assistance to Client as Client may reasonably request (insofar as such information is available to Unmind and the sharing thereof does not compromise the security, confidentiality, integrity or availability of any Personal Data and/or any confidential or commercially sensitive information) to help Client meet its obligations under Applicable Data Protection Laws, including in relation to the security of Client Personal Data, the reporting and investigation of Personal Data Breaches, the demonstration of Client’s compliance with such obligations, and the performance of any ‘data protection impact assessments’ and consultations with Supervisory Authorities or other government authorities regarding such assessments in relation to Unmind’s Processing of Client Personal Data, including those required under Articles 35 and 36 of the GDPR.

9.2 Subject to Section 9.4 below, Unmind shall make available to Client such information as Client may reasonably request for Unmind to demonstrate its compliance with Applicable Data Protection Laws and this DPA. Without limitation of the foregoing, Client may conduct (in accordance with Section 9.3), at its sole cost and expense, and Unmind will reasonably cooperate with, reasonable audits (including inspections, manual reviews, and automated scans and other technical and operational testing that Client is entitled to perform under Applicable Data Protection Laws), in each case, whereby Client or a qualified and independent auditor appointed by Client using an appropriate and accepted audit control standard or framework may audit Unmind’s technical and organisational measures in support of such compliance and the auditor’s report is provided to Client and Unmind upon Client’s request. Nothing in this Section 9 shall be construed to obligate Unmind to breach any duty of confidentiality.

9.3 Client shall give Unmind reasonable advance notice of any such audits. The audit must be conducted in accordance with Unmind’s safety, security or other relevant policies, must not impact the security, confidentiality, integrity or availability of any data, information or materials Processed by Unmind, and must not unreasonably interfere with Unmind’s business activities. Client shall not conduct any scans or technical or operational testing of Unmind’s applications, websites, services, networks or systems without Unmind’s prior approval (which shall not be unreasonably withheld). Unmind need not cooperate with any audit:

(a) performed by any individual or entity who has not entered into a non-disclosure agreement with Unmind on terms acceptable to Unmind in respect of information obtained in relation to the audit;

(b) conducted outside of Unmind’s normal business hours at the relevant site; or

(c) on more than one (1) occasion in any calendar year during the term of the Agreement, except for any additional audits that Client is required to perform under Applicable Data Protection Laws.

9.4 If the controls or measures to be assessed in the requested audit are assessed in a SOC 2 Type 2, ISO, NIST or similar audit report performed by a qualified and independent third-party auditor pursuant to a recognised industry standard audit framework within twelve (12) months of Client’s audit request ("Audit Report") and Unmind has confirmed in writing that there have been no known material changes to the controls audited and covered by such Audit Report(s), Client agrees to accept provision of such Audit Report(s) in lieu of requesting an audit of such
controls or measures. Unmind shall provide copies of any such Audit Reports to Client upon request.

9.5 Audit Reports and any other information obtained by Client in connection with an audit under this Section 9 shall constitute the confidential information of Unmind, which Client shall use only for the purposes of confirming compliance with the requirements of this DPA or meeting Client’s obligations under Applicable Data Protection Laws.

9.6 Client shall reimburse Unmind for any costs reasonably incurred by Unmind in performing its obligations under this Section 9, except to the extent that such costs were incurred as a result of any breach by Unmind of its obligations under this DPA.

10. CLIENT’S RESPONSIBILITIES

Client agrees that, without limiting Unmind’s obligations under Section 5 (Security), Client is solely responsible for its use of the Services, including:

(a) making appropriate use of the Services to maintain a level of security appropriate to the risk in respect of the Client Personal Data;

(b) securing the account authentication credentials, systems and devices Client uses to access the Services;

(c) securing Client’s systems and devices that Unmind uses to provide the Services; and

(d) backing up Client Personal Data on a regular basis.

11. RETURN AND DELETION

11.1 Subject to Section 11.4, upon the date of cessation of any Services involving the Processing of Client Personal Data (the “Cessation Date”), Unmind shall promptly cease all Processing of Client Personal Data for any purpose other than for storage or as otherwise permitted or required under this DPA.

11.2 Client hereby acknowledges and agrees that, due to the nature of the Client Personal Data Processed by Unmind, return (as opposed to deletion) of Client Personal Data is not a reasonably practicable option in the circumstances. Having regard to the foregoing, Client agrees that (for the purposes of Article 28(3)(g) of the GDPR) it is hereby deemed (at the Cessation Date) to have irrevocably selected deletion, in preference of return, of Client Personal Data.

11.3 To the fullest extent technically possible in the circumstances, within thirty (30) days after the Cessation Date, Unmind shall either (at its option) delete or irreversibly anonymise all Client Personal Data then within Unmind’s possession.

11.4 Unmind and any Sub-Processor may retain Client Personal Data where required by applicable law, for such period as may be required by such applicable law, provided that Unmind and any such Sub-Processor shall ensure:

(a) the confidentiality of all such Client Personal Data; and

(b) that such Client Personal Data is only Processed as necessary for the purpose(s) specified in the applicable law requiring its storage and for no other purpose.

12. EEA AND UK RESTRICTED TRANSFERS

12.1 Client acknowledges and agrees that Unmind may store and Process Client Personal Data outside the EEA or the UK. The Parties agree that, to the extent the Client’s transfer of Client Personal Data to Unmind results in a Restricted Transfer:
(a) In the event of an EEA Restricted Transfer, the Parties shall comply with their respective obligations set out in the SCCs, which are hereby deemed to be: (i) populated in accordance with Part 1 of Annex 2 (Population of SCCs); and (ii) entered into by the Parties and incorporated by reference into this DPA; and

(b) In the event of a UK Restricted Transfer, the Parties shall comply with their respective obligations set out in the SCCs, which are hereby deemed to be: (i) varied to address the requirements of the UK GDPR in accordance with UK Transfer Addendum; (ii) populated in accordance with Part 2 of Annex 2 (Population of SCCs); and (iii) entered into by the Parties and incorporated by reference into this DPA.

13. **CONTROLLER DATA**

Client acknowledges and agrees that Unmind shall be a Controller of any Personal Data provided by Data Subjects directly to Unmind, including in connection with their creation of an account with Unmind and/or their use of the Services, and may independently determine the purposes and means of its Processing of such Personal Data.

14. **ORDER OF PRECEDENCE**

In the event of any conflict or inconsistency between:

(a) this DPA and the Agreement, this DPA shall prevail; or

(b) any SCCs entered into pursuant to Section 12 and this DPA, the SCCs shall prevail.

15. **GENERAL**

15.1 This DPA shall be incorporated into and form part of the Agreement with effect on and from the Addendum Effective Date.

15.2 Each Party’s liability under, or in connection with, this DPA shall be subject to the exclusions and limitations of liability set out in the Agreement.

15.3 Unmind may vary this DPA from time to time in its sole discretion, including (without limitation) where Unmind considers it necessary to address the then-current requirements or Applicable Data Protection Laws. Unmind will notify Client in writing of any revisions to this DPA, and any such revisions shall become effective immediately on written notice to Client.
Annex 1

Details of Processing

Note:
This Annex includes certain details of the Processing of Client Personal Data by Unmind as required by Article 28(3) GDPR.

SUBJECT MATTER AND DURATION OF THE PROCESSING OF CLIENT PERSONAL DATA

The subject matter and duration of the Processing of the Client Personal Data are set out in the Agreement and the DPA.

THE NATURE AND PURPOSE OF THE PROCESSING OF CLIENT PERSONAL DATA

1. Processing of user management data. (Eligibility data)

1.2 Assessment of eligibility and user eligibility management

Personal Data comprised within eligibility lists (see 2.1 below) to be provided by Client to Unmind at regular intervals, identifying those of its Personnel who are joining and leaving its employment or engagement, and who are therefore eligible, or ceasing to be eligible, as applicable, to access the Unmind Platform made available to such Personnel pursuant to the Agreement. Access is removed no later than thirty (30) days after receipt by Unmind of notification of the cessation of such employment or engagement.

1.2 Eligible and existing user engagement communications

Unmind will Process Personal Data comprised within eligibility lists (see 2.1 below) on Client’s behalf to send communications to:

- those Client Personnel who are eligible to access the Unmind Platform, but have not yet registered, informing them of their eligibility and providing details of how to register for an account on the Unmind platform;

- Client Personnel on such eligibility lists to share ‘learning and development’ content that such Client Personnel are required or requested by client to complete or view with their employment at the Client; and

- Client Personnel concerning their level of utilisation of content and other offerings available to them on the Unmind platform.

Such communications shall be made in accordance with the provided schedule of work (SOW) agreed between the Parties. Unmind shall provide an ‘UNSUBSCRIBE’ link in each such communication and manage a suppression list on Client’s behalf.

2. Processing of Employee Data

Advanced reporting requires supplying additional employee data (see 2.2 below). This additional data will provide Client Administrators with the ability to segment Unmind Index and engagement data across a range of demographics in their business to inform the effectiveness of targeted wellbeing strategies.

Additional employee data will also be used to create a more personalised experience for each user, in turn improving the overall engagement and efficacy of the Unmind Platform, enabling frictionless user management for Client Administrators for greater reporting accuracy.
CLIENT PERSONAL DATA TO BE PROCESSED

2.1 Processing of eligibility data

- First Name (required)
- Last Name (required)
- Email address (required)
- Unique or Employee ID (required if applicable)
- Line Manager status (optional - based on package)

2.2 Processing of employee data

- Department or Team (required)
- Location (required)
- Manager’s ID (optional)
- Employment Start Date (optional)
- Employment Termination Date (optional)
- Gender (optional)
- Age (optional)
- Time Off Requests (optional – e.g. vacation, sick, personal, jury duty, volunteer, bereavement)
- Time Off (optional)
- Time Off Balance (optional)
- Ethnicity (optional)
- Employment type (optional – type of employment e.g. permanent or contractor)

THE CATEGORIES OF DATA SUBJECT TO WHOM THE CLIENT PERSONAL DATA RELATES

Client Personnel

THE OBLIGATIONS AND RIGHTS OF CLIENT

The obligations and rights of Client are set out in the Agreement and the DPA.
Annex 2

Population of SCCs

Notes:

- In the context of any EEA Restricted Transfer, the SCCs populated in accordance with Part 1 of this Annex are incorporated by reference into, and form an effective part of, this DPA.

- In the context of any UK Restricted Transfer, the SCCs as varied by the UK Transfer Addendum and populated in accordance with Part 2 of this Annex are incorporated by reference into, and form an effective part of, this DPA.

PART 1: EEA RESTRICTED TRANSFERS

1. SIGNATURE OF THE SCCs

Where the SCCs apply in accordance with Section 12 of this DPA, each Party is hereby deemed to have signed the SCCs at the relevant signature block in Annex I to the Appendix to the SCCs.

2. MODULE

Module Two (Controller to Processor) of the SCCs shall apply to any EEA Restricted Transfer.

3. POPULATION OF THE BODY OF THE SCCs

3.1 The SCCs shall be populated as follows:

(a) The optional ‘Docking Clause’ in Clause 7 is not used and the body of that Clause 7 is left intentionally blank.

(b) In Clause 9:

(i) OPTION 2: GENERAL WRITTEN AUTHORISATION applies, and the minimum time period for advance notice of the addition or replacement of Sub-Processors shall be the advance notice period set out in Section 8 of this DPA; and

(ii) OPTION 1: SPECIFIC PRIOR AUTHORISATION is not used and that optional language is deleted; as is, therefore, Annex III to the Appendix to the SCCs.

(c) In Clause 11, the optional language is not used and is deleted.

(d) In Clause 13, all square brackets are removed and all text therein is retained.

(e) In Clause 17: OPTION 1 applies, and the Parties agree that the SCCs shall be governed by the laws of Ireland in relation to any EEA Restricted Transfer; and OPTION 2 is not used and that optional language is deleted.

(f) For the purposes of Clause 18, the Parties agree that any dispute arising from the SCCs in relation to any EEA Restricted Transfer shall be resolved by the courts of Ireland, and Clause 18(b) is populated accordingly.

4. POPULATION OF ANNEXES TO THE SCCs
4.1 Annex I to the Appendix to the SCCs is populated with the corresponding information detailed in Annex 1 (*Details of Processing*), with Client being ‘data exporter’ and Unmind being ‘data importer’.

4.2 Part C of Annex I to the Appendix to the SCCs is populated as below:

*Data Protection Commission*

21 Fitzwilliam Square South

Dublin 2

D02 RD28

Ireland

4.3 Annex II to the Appendix to the SCCs is populated by reference to the Security Measures.

**PART 2: UK RESTRICTED TRANSFERS**

Where relevant in accordance with Section 12 of this DPA, the SCCs also apply in the context of UK Restricted Transfers as varied by the UK Transfer Addendum in the manner described below:

(a) **Part 1 of the UK Transfer Addendum.** As permitted by Section 17 of the UK Transfer Addendum, the Parties agree that:

(i) Tables 1, 2 and 3 of Part 1 of the UK Transfer Addendum are deemed populated with the corresponding details set out in Annex 1 (*Details of Processing*) and the foregoing provisions of Part 1 of this Annex (subject to the variations effected by the Mandatory Clauses described in (b) below); and

(ii) Table 4 of Part 1 of the UK Transfer Addendum is completed by the box labelled ‘Data Importer’ being deemed to have been ticked.

(b) **Part 2 of the UK Transfer Addendum.** The Parties agree to be bound by the Mandatory Clauses of the UK Transfer Addendum.

In relation to any UK Restricted Transfer to which they apply, where the context permits and requires, any reference in this DPA to the SCCs shall be read as a reference to those SCCs as varied in the manner set out in this Part 2.
Annex 3

California and Virginia Annex

1. In this Annex, the terms “business,” “business purpose,” “commercial purpose,” “consumer,” “sell,” “share,” and “service provider” shall have the respective meanings given thereto in the CCPA, and “personal information” shall mean Client Personal Data that constitutes “personal information” or “personal data” as defined in and that is subject to the CCPA or CDPA (the CCPA and CDPA collectively the “State Privacy Laws”).

2. The business purposes and services for which Unmind is Processing personal information are for Unmind to provide the services to and on behalf of Client as set forth in the Agreement, as described in more detail in Annex 1 (Details of Processing).

3. It is the Parties’ intent that with respect to any personal information, Unmind is a service provider. Unmind (a) acknowledges that personal information is disclosed by Client only for limited and specific purposes described in the Agreement; (b) shall comply with applicable obligations under the State Privacy Laws and shall provide the same level of privacy protection to personal information as is required by the State Privacy Laws; (c) agrees that Client has the right to take reasonable and appropriate steps under Section 9.1 of the DPA to help ensure that Unmind’s use of personal information is consistent with Client’s obligations under the State Privacy Laws; (d) shall notify Client in writing of any determination made by Unmind that it can no longer meet its obligations under the State Privacy Laws; and (e) agrees that Client has the right, upon notice, including pursuant to the preceding clause, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.

4. Unmind shall not (a) sell or share any personal information; (b) retain, use or disclose any personal information for any purpose other than for the business purposes specified in the Agreement, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purpose specified in the Agreement, or as otherwise permitted by the State Privacy Laws; (c) retain, use or disclose the personal information outside of the direct business relationship between Unmind and Client; or (d) combine personal information received pursuant to the Agreement with personal information (i) received from or on behalf of another person, or (ii) collected from Unmind’s own interaction with any consumer to whom such personal information pertains. Unmind hereby certifies that it understands its obligations under this Paragraph 3 and will comply with them.

5. Unmind shall implement reasonable security procedures and practices appropriate to the nature of the personal information received from, or on behalf of, Client, in accordance with Section 5 of the DPA.

6. When Unmind engages any Sub-Processor, Unmind shall notify Client of such Sub-Processor engagements in accordance with Section 8 of the DPA and that such notice shall satisfy Unmind’s obligation under the State Privacy Laws to give notice of and an opportunity to object to such engagements.

7. Unmind agrees that Client may conduct audits, in accordance with Section 9 of the DPA, to help ensure that Unmind’s use of personal information is consistent with Unmind’s obligations under the State Privacy Laws.

8. The Parties acknowledge that Unmind’s retention, use and disclosure of personal information authorized by Client’s instructions documented in the Agreement and DPA are integral to Unmind’s provision of the Services and the business relationship between the Parties.

8. Unmind agrees to cooperate in good faith with Client to further amend the Agreement or DPA as may be necessary to address compliance with the State Privacy Laws.
Annex 4

Security Measures

As from the Addendum Effective Date, Unmind will implement and maintain the Security Measures as set out in this Annex.

Unmind maintains a company-wide information security management system (ISMS) and control program that includes written security policies, standards and procedures based upon and in adherence with Unmind’s ISO 27001 certification. This ISMS will help protect Client Personal Data against accidental, unauthorised, or unlawful access, disclosure, alteration, loss, or destruction.

Unmind may modify any of its policies, process, or procedures at any time and without obligation to notify or update this Annex, provided such modifications provide substantially similar or greater protections than those provided for herein.

Access Controls

Unmind implements Industry Standard access control methodologies, which rely on policy, process, and logical controls to help prevent unauthorised access to systems and data under Unmind’s control. These access controls include no less than the following:

- Unmind uses the “Principle of Least Privilege” model for restricting access to systems and data and adheres to a strict access rights review schedule to ensure regular review of access permissions for all systems.

- Unmind Personnel each have a unique user ID and personal secret password for accessing internal networks, applications, and data. Unmind shall maintain policies concerning the maintenance of password management as per the ISO 27001 requirement.

- Unmind will suspend access to all Unmind systems and data within twenty-four hours of employment termination and modify permissions within forty-eight hours in instances of role or responsibility change.

- Unmind maintains a password complexity policy that requires:
  - Minimum password length is 12 characters
  - Require at least one uppercase letter from Latin alphabet (A-Z)
  - Require at least one lowercase letter from Latin alphabet (a-z)
  - Require at least one number
  - Allow users to change their own password
  - Remember last 5 password(s) and prevent reuse

- Multi-factor authentication is used for all systems containing critical data. All passwords must be stored and transmitted using Encryption Standards.

- Physical office locations will have appropriate physical security measures in place, including but not limited to, electronic access controls, visitor procedures, intruder detection and video surveillance.

Encryption of Data

Encryption algorithms that are publicly or commercially available shall be utilised both at rest and in transit with key lengths sufficient to prevent commercially reasonable attempts to decrypt through brute force the encrypted information.

Key management will be established via Unmind’s Cryptography Policy and shall protect keys against unauthorised access, misuse and security incidents.
Secure Software Practice

Unmind shall implement and conform its software development practices to applicable Industry Standards. Unmind will maintain a secure server environment where physical and logical security controls are in place as well as disaster recovery capabilities and redundancy processes;

- Use commercially reasonable measures to detect product vulnerabilities prior to release. These measures may include manual test scripts, test automation, dynamic code analysis, static code analysis, or other measures chosen by Verint.

- Unmind will carry out an annual independent technical security assessment and penetration testing service to identify any areas of vulnerability of the Unmind Platform in addition to identifying a threat of unauthorised access.

- Unmind shall update procedures and processes from time to time to improve detection of vulnerabilities within its products.

- Unmind’s developers shall receive training where required on coding and design with respect to application security.

Incident Management and Business Continuity

Unmind will maintain an incident management plan and business continuity policy which define roles and responsibilities on proper handling of information security events. Documentation will include a plan intended to facilitate the restoration of critical operations and processes which would allow for Unmind’s continued performance of its obligations. Business continuity and incident management plans will be tested, reviewed, and updated as required annually.

Logging and Monitoring

Unmind will deploy tools that monitor and log

- Application Security
- Container Security
- File Storage Security
- Network Security
- Workload Security
- Conformity

Tools will be used to ensure complete visibility of all aspects of the platform and shall be monitored by the Infrastructure team.

Security and Awareness Training

Unmind shall provide all employees and contractors with mandatory Information Security training and awareness modules and maintain training completion records in line with relevant industry standard and best practice retention policies.

Human Resources

Performance of background checks, as well as execution of non-disclosure commitments prior to employment and acknowledgment of information security policies is required for all Unmind employees and contractors.

Security Audit

Unmind conducts internal and external third-party audits on a regularly scheduled basis. Unmind shall correct any non-conformities noted in an audit report within the relevant timeframe and shall request auditor to provide an updated report reflecting successful corrective actions.
Client may request executive summaries of these audit reports. Unmind reserves the right to redact confidential information from these reports prior to sharing with Client.

Unmind may freely update or modify these Security Measures from time to time provided that such updates and modifications do not decrease the overall security of Client Personal Data.
Annex 5

Authorised Sub-Processors of client personal data.

<table>
<thead>
<tr>
<th>Sub-Processor</th>
<th>Description of Data Processing Services</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Web Services</td>
<td>Third-party hosting provider</td>
<td>Republic of Ireland in the eu-west-1 Region.</td>
</tr>
<tr>
<td>Braze</td>
<td>User engagement platform</td>
<td>AWS EU-Central 1.</td>
</tr>
<tr>
<td>Mailchimp/Mandrill</td>
<td>Email delivery provider</td>
<td>United States.</td>
</tr>
<tr>
<td>Twilio/Segment</td>
<td>Customer Data Platform</td>
<td>AWS US West (Oregon) Region.</td>
</tr>
<tr>
<td>Merge.dev</td>
<td>API provider for HRIS integration</td>
<td>Multi region and can be selected to comply with regional requirements.</td>
</tr>
<tr>
<td>Auth0</td>
<td>Platform Identity and Access Management solution</td>
<td>European Union.</td>
</tr>
</tbody>
</table>