EXHIBIT B
MENTORCLIQ DATA PROCESSING ADDENDEUM ("DPA")

This MentorcliQ Data Processing Addendum, including its Standard Contractual Clauses adopted by the European Commission, ("DPA"), forms part of the MentorcliQ Master Subscription Agreement, Terms of Service or other written or electronic agreement between the parties, and reflects the parties' agreement with respect to the terms governing the Processing of Personal Data under the MentorcliQ Master Subscription Agreement and associated Services Order or Statement of Work (the "Agreement"). This DPA is an addendum to that Agreement and is effective upon Client's signature to the Agreement and is incorporated into the Agreement, which incorporation may be specified in the Agreement, an Order or an executed amendment to the Agreement.

The term of this DPA shall follow the term of the Agreement. Terms not otherwise defined herein shall have the meaning as set forth in the Agreement.

1. Definitions

"CCPA" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations.

"Client" means the entity that executed the Agreement and for which Personal Data is being Processed by MentorcliQ.

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

"Data Protection Law" means all applicable legislation relating to data protection and privacy including laws and regulations of the European Union, The European Economic Area, and their member states, Switzerland, the United Kingdom and the United States and its states to the extent applicable to the Processing of Personal Data under this Agreement, as amended, repealed, consolidated, or replaced from time to time.

"Data Subject" means the identified or identifiable person to whom Personal Data relates.

"GDPR" means the Regulation (EU) 23016/679 of the European Parliament and of the Council of 27 April 21016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), including as implemented or adopted under the laws of the United Kingdom.

"Instruction" means the written, documented instruction, issued by Controller to Processor, and directing them to perform a specific action with regard to Personal Data (including, but not limited to, anonymizing, blocking, deletion, making available).

"Personal Data" means any information relating to an identified or identifiable individual where such information is contained within Client Data and is protected similarly as personal data or personally identifiable information under applicable Data Protection Law

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.

"MentorcliQ Mentoring Platform" means the object code version of the computer software application(s) owned by or licensed to MentorcliQ that is made available, through an internet address or otherwise, by MentorcliQ or its agents to Controller in connection with this Agreement, together with any associated Materials. The Platform also includes any upgrades, improvements, bug fixes, new versions and/or derivative works of such software or Materials.

"Processing" means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, or erasure of Personal Data.

"Processor" means a natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of the Controller, including, any "service provider" as that term is defined by the CCPA.

"Special Data" means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

"Standard Contractual Clauses" means the clauses attached hereto as Schedule 1 pursuant to the European Commission's decision (C(2010)593) of 4 June 2021 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

"Sub-Processor" means any Processor engaged by MentorcliQ.

2. Details of the Processing

a. Categories of Data Subjects. Data Subjects consist of participants/employees and administrators/employers involved in mentoring initiatives, utilizing the MentorcliQ Mentoring Platform and associated Services.

b. Types of Personal Data. The types of data collected include contact details (such as name, email address), professional information (such as job title, job function, company, company address), mentoring preferences, responses to personality questionnaire(s), profile picture, a link to data subject's public LinkedIn profile page, demographic data, progress in and satisfaction with the program(s) via responses to short

surveys, as well as any information voluntarily provided in the course of using the MentorcliQ Help Center forums. Controller may wish to track Diversity and Inclusion metrics and so may choose to collect Race/Ethnicity. This would be categorized as Special Data. All data fields are optional and at the Controller's discretion.

c. Subject-Matter and Nature of the Processing. The subject-matter of Processing of Personal Data by Processor is the performance of the Services pursuant to the Agreement as specified in the Agreement and any applicable Order or Statement of Work.

d. Purpose of the Processing. Personal Data will be Processed for purposes of providing a configured instance of the MentorcliQ Mentoring Platform and associated Services set out and otherwise agreed to in the Agreement and any applicable Order or Statement of Work.

e. Duration of the Processing. Personal Data will be Processed for the duration of the Agreement, subject to Section 4 of this DPA.

3. Obligations of Data Controller

The Data Controller agrees that it shall ensure that any disclosure of Personal Data made by it to the Data Processor is made with the Data Subject's consent, via a legitimate basis as provided for in the GDPR, or is otherwise lawful in compliance with the Data Protection Law. Data Controller specifically acknowledges that its use of the Services will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Personal Data, to the extent applicable under the CCPA.

4. Obligations of Processor

MentorcliQ shall treat Personal Data as Confidential Information and shall only Process Personal Data on behalf of and in accordance with Controller's documented instructions for the following purposes: (a) Processing in accordance with the Agreement and applicable Order Form(s) or Statement(s) of Work; (b) Processing initiated by Data Subjects in their use of the Services; and (c) Processing to comply with other documented reasonable instructions provided by Controller (e.g., via email) where such instructions are consistent with the terms of the Agreement and otherwise lawful.

Processor shall take the appropriate technical and organizational measures to adequately protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, described under Schedule 2 to the Standard Contractual Clauses.

Processor will facilitate Controller's compliance with the Controller's obligation to implement security measures with respect to Personal Data (including if applicable Controller's obligations pursuant to Articles 32 to 34 (inclusive) of the GDPR), by implementing and maintaining the security measures described under Annex II, complying with the terms relation to Personal Data Breaches below; and providing the Controller with information in relation to the Processing in accordance with Section 5 (Audits).

Processor shall ensure that any personnel whom Processor authorizes to process Personal Data on its behalf has received appropriate training on their responsibilities and is subject to confidentiality obligations with respect to that Personal Data. The undertaking to confidentiality shall continue after the termination of the Agreement. Processor shall ensure that its access to the Personal Data is limited to those personnel performing Services in accordance with the Agreement.

Processor will notify the Controller within 48 hours after it becomes aware of any of any Personal Data Breach affecting any Personal Data. Processor will provide the Controller with all reasonable assistance necessary to enable the Controller to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if Controller is required to do so under the Data Protection Law.

Processor shall be entitled to engage Sub-Processors to fulfil Processor's obligations defined in the Agreement only with Controller's written consent. For these purposes, Controller consents to the engagement as sub-Processors of Processor's affiliated companies and the third parties listed in Annex III. For the avoidance of doubt, the above authorization constitutes Controller's prior written consent to the Sub-Processing by Processor for purposes of Clause 7.7 of the Standard Contractual Clauses.

Where Processor engages Sub-Processors, Processor will enter into a contract with the Sub-Processor that imposes on the Sub-Processor the same obligations that apply to Processor under this DPA. Where the Sub-Processor fails to fulfil its data protection obligations, Processor will remain liable to the Controller for the performance of such Sub-Processors obligations.

Controller acknowledges and agrees that, in connection with the performance of the Services under the Agreement, Personal Data will be transferred to MentorcliQ in the United States, unless otherwise specified in applicable Order Form(s) or Statement(s) of Work. MentorcliQ. Is a part of the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks, in order to implement appropriate safeguards for such transfers pursuant to Article 46 of the GDPR. The Standard Contractual Clauses at Schedule 2 will apply with respect to Personal Data that is transferred outside the EEA, either directly or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the Data Protection Law).

Other than to the extent required to comply with Data Protection Law, following termination or expiry of the Agreement, Processor will return data to the Controller in a mutually agreeable format (e.g. .csv flat-file) and delete all Personal Data (including copies thereof) Processed pursuant to this DPA.

5. Audits

Controller may, prior to the commencement of Processing, and at regular intervals thereafter, audit the technical and organizational measures taken by Processor. Processor shall, upon Controller's written request and within a reasonable period of time, provide Controller with

information necessary for such audit, to the extent that such information is within Processor's control and Processor is not precluded from disclosing it by applicable law, a duty of confidentiality, or any other obligation owed to a third party.

6. Data Subject Rights

MentorcliQ shall, to the to the extent legally permitted, promptly notify Controller if MentorcliQ receives 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, each such request being a "Data Subject Request". Taking into account the nature of the Processing, MentorcliQ shall assist Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Controller's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Controller, in its use of the Services, does not have the ability to address a Data Subject Request, MentorcliQ shall upon Controller's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent MentorcliQ is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws. To the extent legally permitted, Controller shall be responsible for any costs arising from MentorcliQ 's provision of such assistance.

7. General Provisions

Effective 25 May 2018, MentorcliQ will Process Personal Data in accordance with the GDPR requirements contained herein which are directly applicable to MentorcliQ's provision of the MentorcliQ Mentoring Platform and associated Services.

List of Schedules

Schedule 1: Transfer Mechanisms for European Data Transfers

Schedule 2: Standard Contractual Clauses

SCHEDULE 1: Transfer Mechanisms for European Data Transfers

1. Introduction. The Standard Contractual Clauses and the additional terms specified in this Schedule 1 apply to (i) Client, which is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom and, (ii) its Authorized Affiliates. For the purpose of the Standard Contractual Clauses, the aforementioned entities shall be deemed "data exporters".
2. Instructions. This DPA and the Agreement are Client's complete and final documented instructions at the time of signature of the Agreement to MentorcliQ for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of the Standard Contractual Clauses, the following is deemed an instruction by the Client to process Personal Data: (a) Processing in accordance with the Agreement and applicable Statements of Work; and (b) Processing to comply with other reasonable documented instructions provided by Client (e.g., via email) where such instructions are consistent with the terms of the Agreement.
3. Data Exports from the United Kingdom under the Standard Contractual Clauses. In case of any transfers of Personal Data under this DPA under the Standard Contractual Clauses from the United Kingdom, to the extent such transfers are subject to Data Protection Laws and Regulations applicable in the United Kingdom ("UK Data Protection Laws"), (i) general and specific references in the Standard Contractual Clauses to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 shall hereby be deemed to have the same meaning as the equivalent reference in the UK Data Protection Laws; (ii) References in the Standard Contractual Clauses to "the law of the Member State in which the data exporter is established" shall hereby be deemed to mean "the law of the United Kingdom"; and (iii) any other obligation in the Standard Contractual Clauses determined by the Member State in which the data exporter is established shall hereby be deemed to refer to an obligation under UK Data Protection Laws.
4. Notification of New Sub-processors and Objection Right for new Sub-processors. Pursuant to Clause 7.7 of the Standard Contractual Clauses, Client acknowledges and expressly agrees that MentorcliQ may engage new Sub-Processors as described in Section 4 of the DPA.
5. Copies of Sub-processor Agreements. The parties agree that the copies of the Sub-Processor agreements that must be provided by MentorcliQ to Client pursuant to the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by MentorcliQ beforehand; and, that such copies will be provided by MentorcliQ, in a manner to be determined in its discretion, only upon request by Customer.
6. Audits and Certifications. The parties agree that the audits described in the Standard Contractual Clauses shall be carried out in accordance with the following specifications:
    - Client may contact MentorcliQ in accordance with the "Notices" Section of the Agreement to request an on-site audit of the procedures relevant to the protection of Personal Data. Client shall reimburse MentorcliQ for any time expended for any such on-site audit at the MentorcliQ's then-current professional services rates, which shall be made available to Client upon request. Before the commencement of any such on-site audit, Client and MentorcliQ shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Customer shall be responsible. All reimbursement rates shall be reasonable, taking

into account the resources expended by MentorcliQ. Client shall promptly notify MentorcliQ with information regarding any non-compliance discovered during the course of an audit.

- Certification of Deletion. The parties agree that the certification of deletion of Personal Data that is described in the Standard Contractual Clauses shall be provided by MentorcliQ to Client only upon Client's written request.
- Conflict. In the event of any conflict or inconsistency between the body of this DPA and any of its Schedules (not including the Standard Contractual Clauses) and the Standard Contractual Clauses in Schedule 2, the Standard Contractual Clauses shall prevail.

SCHEDULE 2: Standard Contractual Clauses

Standard Contractual Clauses (Processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection,

The Client, as defined in the Agreement (the "data exporter")

and

MentorcliQ, Inc. 595 S. Third Street, 2nd Floor, Columbus, OH 43215 USA (the "data importer"),

each a 'party'; together 'the parties',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Annex II.

SECTION I

Clause 1 - Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of data to a third country.

(b) The Parties: the data exporter and data importer have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2 - Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3 - Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4 - Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5 - Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6 - Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional - Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8 - Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Annex as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Annex to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In

case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex II.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9 - Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 daysin advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10 - Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11 - Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 - Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13 - Supervision

(a) The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14 - Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards.

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15 - Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary, with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16 - Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17 - Governing law

These Clauses shall be governed by the law of the jurisdiction in the member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights.

Clause 18 - Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of (specify Member State).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I - Description of the Processing

This Annex forms part of the Clauses. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Annex.

A. List of Parties

Data exporter: The data exporter is the Client, as defined in the Agreement or Terms of Service Agreement, as applicable, and may be contacted as further set forth in the Agreement or Terms of Service Agreement, as applicable.

Data importer: The data importer is MentorcliQ, Inc., provider of the MentorcliQ Mentoring Platform, and may be contacted as further set forth in the Agreement or Terms of Service Agreement, as applicable.

B. Description of the Transfer

Categories of data subjects whose persons data is transferred:

Client may submit Personal Data to the Services, the extent of which is determined and controlled by Client in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

- Client's employees or agents who the Client has identified to take part in, or potentially take part in, MentorcliQ's mentoring services.

- Client's employees who act as Administrators in registering the Client and/or the Client's employees or agents who may take part in MentorcliQ's mentoring services.

Categories of personal data transferred:

Client or the Data Subject identified above may submit Personal Data to the Services, the extent of which is determined and controlled by Client in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Contact information (company email address)
- Professional information, such as, job title, job functions, employer, office location)
- Mentoring Preferences
- Response to short personality survey
- Profile picture
- Link to Data Subject's public LinkedIn profile page
- Demographic data
- Progress in and satisfaction with MentorcliQ's services
- Localization data
- Information voluntarily provided in the course of using the MentorcliQ Help Center forums

MentorcliQ will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the DPA, and as further instructed by Client in its use of the Services.

Sensitive data transferred and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Client may, subject to the restrictions set out in the Documentation, submit special categories of Personal Data to the Services, the extent of which is determined and controlled by Client in its sole discretion, and which is for the sake of clarity Personal Data with information revealing racial or ethnic origin.

The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis).

The transferred shall occur on a one-off basis., or where optional HRIS integration is employed, at a cadence mutually agreed upon between the Parties, typically weekly.

Nature of processing: MentorcliQ will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the DPA, and as further instructed by Client in its use of the Services.

Purpose of processing: Personal data will be processed for purposes of providing a configured instance of the data importer's Mentoring Platform and associated Services set out and otherwise agreed to in the Agreement and any applicable Order or Statement of Work.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: Subject to Section 2(e) of the DPA, MentorcliQ will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

The subject-matter of Processing of Personal Data by Processor is the provision of the MentorcliQ Mentoring Platform and services to the Exporter and Data Subjects that involves the Processing of Personal Data. Personal Data will be subject to those Processing activities as may be specified in the Agreement and an Order or Statement of Work.

C. Competent Supervisory Authority

The competent supervisory authority is in accordance with Clause 13.

Annex II

Technical and Organizational Measures Including Technical and Organisational Measures to Ensure the Security of the Data

This Annex forms part of the Clauses.

Description of the technical and organizational security measures implemented by the data importer:

MentorcliQ currently observes the security practices described in this Annex II. Notwithstanding any provision to the contrary otherwise agreed to by data exporter, MentorcliQ may modify or update these practices at its discretion provided that such modification and update does not result in a material degradation in the protection offered by these practices. All capitalized terms not otherwise defined herein shall have the meanings as set forth in the Agreement.

a) Access Controls

i) Preventing Unauthorized Product Access

Outsourced processing: MentorcliQ hosts its Service with underlying cloud infrastructure providers. MentorcliQ maintains contractual relationships with vendors in order to provide the Service in accordance with our Data Processing Addendum.

Physical and environmental security: MentorcliQ's underlying data hosting provider possesses the physical and environmental security controls audited for under SOC 2 Type II and ISO 27001 compliance, among other certifications.

Authentication: MentorcliQ utilizes either a password policy for its Mentoring Platform, or a Single-Sign-On (SSO) solution with our clients. In the case of Single-Sign-On, the authentication controls set out by the clients' SSO control authentication security stance. Clients who interact with the Platform via the user interface must authenticate before accessing.

Authorization: Client data is accessible to clients via the MentorcliQ Mentoring Platform. Clients do not directly access the underlying application infrastructure.

ii) Preventing Unauthorized Use

MentorcliQ implements access controls and detection capabilities for the internal networks that support its Client Platforms.

Access controls: MentorcliQ maintains up-to-date firewall rulesets, employs an IPS to detect and prevent unauthorized host access, and utilizes an integrated CDN, which provides WAF-style rules and DDoS protection filtering for each of our sites and environments.

Static code analysis: Security reviews of source code repositories is performed, checking for coding best practices and identifiable software flaws.

Vulnerability Scanning and Penetration Testing: MentorcliQ carries out vulnerability scanning, including automated penetration testing, based on a consistently updated database of exploits provided by a network of white-hat hackers. The intent of the penetration testing is to identify and resolve foreseeable attack vectors and potential abuse scenarios.

iii) Limitations of Privilege & Authorization Requirements

Role-Based Least Privilege Access: MentorcliQ utilizes role-based access according to least privilege, such that only the minimum necessary number of individuals (MentorcliQ Employees and Client Administrators) have access. All access is logged, and roles and privileges are reviewed at least quarterly.

Background Checks: MentorcliQ employees undergo a third-party background check prior to being extended an employment offer, in accordance with the applicable laws. All employees are required to conduct themselves in a manner consistent with company guidelines, confidentiality requirements, and ethical standards.

b) Transmission Control

MentorcliQ applies end-to-end encryption. In transit, HTTPS encryption (also referred to as SSL or TLS) is utilized, using industry standard algorithms and certificates. Backups are encrypted during transfer and at-rest with 256-bit Advanced Encryption Standard ciphers, storing private keys and encrypted backup data on separate servers. 100% of the data on all backup media is encrypted.

c) Input Control

Detection: MentorcliQ logs extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregate log data and alert appropriate employees of malicious, unintended, or anomalous activities. MentorcliQ personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and Tracking: MentorcliQ maintains a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, MentorcliQ will take appropriate steps to minimize product and Client damage or unauthorized disclosure.

Communication: If MentorcliQ becomes aware of unlawful access to Client data stored within its products, MentorcliQ will: 1) notify the affected clients of the incident; 2) provide a description of the steps MentorcliQ is taking to resolve the incident; and 3) provide status updates to the Client contact.

d) Availability Control

Infrastructure Availability: The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.9% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and HVAC services.

Fault Tolerance: Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. All databases are backed up and maintained using at least industry standard methods.

Annex III - List of Sub-Processors

The Controller has authorized the use of the following Sub-Processors:

Google, Inc.

Amazon Web Services, Inc.

Pantheon.io

Note that not all Sub-Processors may apply to Client's instance of the MentorcliQ mentoring platform, but if Sub-Processors are used, they are listed above or, if added later, will be added pursuant to the terms of this DPA.