DATA PROCESSING AGREEMENT

This MentorcliQ Data Processing Agreement ("**DPA**"), that includes the Standard Contractual Clauses adopted by the European Commission, as applicable, reflects the parties' agreement with respect to the terms governing the Processing of Personal Data under the MentorcliQ Terms of Service and associated Services Order or Statement of Work (the "**Agreement**"). This DPA is an amendment to that Agreement and is effective upon its incorporation into the Agreement, which incorporation may be specified in the Agreement, an Order or an executed amendment to the Agreement. Upon its incorporation into the Agreement, the DPA will form a part of 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.

THIS DPA INCLUDES:

(i) Standard Contractual Clauses, attached hereto as **Exhibit 1**.

      (a) **Appendix 1** to the Standard Contractual Clauses, which includes specifics on the Personal Data transferred by the data exporter to the data importer.

      (b) **Appendix 2** to the Standard Contractual Clauses, which includes a description of the technical and organizational security measures implemented by the data importer as referenced.

(ii) List of Sub-Processors, attached hereto as **Exhibit 2**.

1. Definitions

"**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.

"**Data Protection Law**" means all applicable legislation relating to data protection and privacy including without limitation the EU Data Protection Directive 95/46/EC and all local laws and regulations which amend or replace any of them, including the GDPR, together with any national implementing laws in any Member State of the European Union or, to the extent applicable, in any other country, as amended, repealed, consolidated or replaced from time to time.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 General Data Protection 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.

"**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.

"Standard Contractual Clauses" means the clauses attached hereto as Exhibit 1 pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 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.

2. Details of the Processing

a. Categories of Data Subjects. Data Subjects consist of participants and administrators involved in mentoring initiatives, utilizing the MentorcliQ Mentoring Platforml and any associated services.

b. Types of Personal Data. Data fields 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 or Sensitive category of 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 provision of the MentorcliQ Mentoring Platform and associated services to the Controller 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 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 or is otherwise lawful.

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) of 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 Appendix 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 Appendix 2, 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 is subject to confidentiality obligations with respect to that Personal Data. The undertaking to confidentiality shall continue after the termination of the Agreement.

Processor will notify the Controller as soon as practicable after it becomes aware of any of any Personal Data Breach affecting any Personal Data. At the Controller's request, Processor will promptly 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.

MentorcliQ shall, 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 ("Data Subject Request"). 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 Controller 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 and Regulations.

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 Exhibit 2. For the avoidance of doubt, the above authorization constitutes Controller's prior written consent to the sub-Processing by Processor for purposes of Clause 11 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. 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 Exhibit 1 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. 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.

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 (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 Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a)   *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

(b)   '*the data exporter'* means the controller who transfers the personal data;

(c)   *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d)   *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e)   '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f)   *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

---

[1]   Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

Clause 3

Third-party beneficiary clause

1.   The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2.   The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3.   The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4.   The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a)   that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b)   that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c)   that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d)   that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e)   that it will ensure compliance with the security measures;

(f)   that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g)   to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h)   to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i)   that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j)   that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[2]

The data importer agrees and warrants:

(a)   to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b)   that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c)   that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d)   that it will promptly notify the data exporter about:

      (i)   any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

      (ii)   any accidental or unauthorised access, and

      (iii)   any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e)   to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f)   at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g)   to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h)   that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i)   that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j)   to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

---

[2]   Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

    The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

    (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

    (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely Luxembourg.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1.   The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[3]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2.   The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3.   The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4.   The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1.   The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2.   The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

---

[3]   This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

APPENDIX 1 to the Standard Contractual Clauses

This Appendix 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 Appendix.

A. Data exporter

The data exporter is the Client, as defined in the MentorcliQ's Master Subscription Agreement ("**Agreement**").

B. Data importer

The data importer is MentorcliQ, Inc., provider of the MentorcliQ Mentoring Solution.

C. Data subjects

Data Subjects consist of participants and administrators involved in mentoring initiatives, utilizing the MentorcliQ Mentoring Solution and any associated services. Typically this is a sub-set of the Data Exporters employees.

D. Categories of data

Data fields 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.

E. Special categories of data (if appropriate)

The parties do not anticipate the transfer of special categories of data. However, Exporter may wish to track Diversity and Inclusion metrics and so may choose to collect Race/Ethnicity. This would be categorized as Special or Sensitive category of Data. All data fields are optional and at the Exporter's discretion.

F. Processing operations

The subject-matter of Processing of Personal Data by Processor is the provision of the MentorcliQ Mentoring Solution 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.

mentorcliQ™

Appendix 2 to the Standard Contractual Clauses

This Appendix 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 Appendix 2. 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 Control

      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 Agreement.

      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 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.

EXHIBIT 2

List of Sub-Processors

Google, Inc.

Amazon Web Services, Inc.

Pantheon.io