

## Data Processing Agreement

This Data Processing Agreement ("Agreement") is made and entered into as of the date of last signature below ("Effective Date") by and between Client (on behalf of itself and its affiliates detailed in Appendix 3 hereto, hereinafter referred to as "Client", "Data Exporter" or "Controller") and Predictive Index, LLC (referred to as "Predictive Index," "Data Importer" or "Processor") in the execution block below (each, a "Party" and together, the "Parties"). This Data Processing Agreement is a supplement to, and made a part of the PI Client Agreement between Controller and Processor.

### HOW TO EXECUTE THIS AGREEMENT:

1. This Agreement and The Standard Contractual Clauses in Annex A have been presigned on behalf of Predictive Index.
2. To complete this Agreement, Client must:
  - a. Complete the information in the signature box and sign on Pages 3, 8, 10, and 11.
  - b. Complete the information in Appendix 3 to The Standard Contractual Clauses on Page 13, if applicable.
3. Send the completed and signed Agreement to Predictive Index by email, indicating the Client Name, and Agreement date, and Agreement ID number (as set out on the applicable Predictive Index Client Agreement), to [privacy@predictiveindex.com](mailto:privacy@predictiveindex.com).

Upon receipt of the validly completed Agreement by Predictive Index at this email address, this Agreement will become legally binding.

### HOW THIS AGREEMENT APPLIES

If the Client entity signing this Agreement is a party to a PI Client Agreement with Predictive Index, this Agreement is an addendum to and forms part of the PI Client Agreement.

If the Client entity signing this Agreement is not a party to a PI Client Agreement, this Agreement is not valid and is not legally binding. Such entity should request that the Client entity who is a party to the PI Client Agreement executes this Agreement.

If the Client entity signing the Agreement is not a party to a PI Client Agreement that includes Predictive Index as a contracting party, but instead includes an authorized reseller of Predictive Index products and services (or "PI Certified Partner") as the contracting party, this Agreement is not valid and is not legally binding. Such entity should contact the authorized reseller or PI Certified Partner to discuss whether any amendment to its agreement with that reseller, or a new PI Client Agreement with Predictive Index, may be required.

This Agreement shall not replace any comparable or additional rights relating to Processing of Data contained in Client's PI Client Agreement (including any existing data processing addendum to the PI Client Agreement).

### 1. DEFINITIONS

All capitalized terms used in this Agreement shall have the meanings given to them below:

**1.1 Applicable Data Protection Law:** means all applicable international, federal, national and state privacy and data protection laws that apply to the processing of Personal Data that is the subject matter of the Agreement (including, where applicable, European Data Protection Law).

**1.2 Controller:** means the entity that determines the purposes and means of the processing of Personal Data, and for the purposes of this Agreement means Client.

**1.3 European Data Protection Law:** means: (i) prior to 25 May 2018, the EU Data Protection Directive 95/46/EC, and any applicable national implementation of it; and (ii) on and after 25 May 2018, the EU General Data Protection Regulation 2016/679 ("GDPR") and any applicable national

laws made under the GDPR.

**1.4 Personal Data:** means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**1.5 Processor:** means an entity that processes Personal Data on behalf of the Controller, and for the purposes of this Agreement means Predictive Index, LLC.

**1.6 Standard Contractual Clauses:** means the standard contractual clauses for the transfer of personal data to processors established in third countries, pursuant to the European Commission Decision C(2010)593, as attached at Annex A.

## 2. DATA PROTECTION

**2.1 Relationship of the Parties:** As between the Parties, Client is the Controller and appoints The Predictive Index as a Processor to process the Personal Data described in Appendix I to Annex A (the "Data").

**2.2 Purpose limitation:** Processor shall process the Data as a Processor only for the purposes described in Appendix I to Annex A, and strictly in accordance with the documented instructions of Client (the "Permitted Purpose"). In no event shall Processor process the Data for its own purposes or those of any third party.

**2.3 International transfers of Data:** Processor will at all times provide an adequate level of protection for the Data, wherever processed, in accordance with the requirements of Applicable Data Protection Law. Processor shall not process or transfer any Data originating from the European Economic Area (EEA) in or to a territory which has not been designated by the European Commission as providing an adequate level of data protection unless [(i)] it has first obtained Client's prior written consent[; and (ii) it executes and complies with its obligations under the Standard Contractual Clauses attached at Annex A (including its Appendices), which shall form an integral part of this Agreement]. By executing this Agreement, Client understands and agrees that Processor is a company located in the United States, and the Personal Data will be processed in the United States and consents to such processing. Processor complies with and has certified to the US-EU Privacy Shield Framework and shall maintain such certification throughout the term of this Agreement. In the event of any conflict between the Standard Contractual Clauses and this Agreement, the Standard Contractual Clauses shall control and supersede.

**2.4 Confidentiality of processing:** Processor shall keep strictly confidential all Personal Data that it processes on behalf of Client. Processor shall ensure that any person that it authorises to process the Data (including Processor's staff, agents and subcontractors) (each an "Authorised Person") shall be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty), and shall not permit any person to process the Data who is not under such a duty of confidentiality. Processor shall ensure that only Authorised Persons will have access to, and process, the Data, and that such access and processing shall be limited to the extent strictly necessary to achieve the Permitted Purpose. Processor accepts responsibility for any breach of this Agreement caused by the act, error or omission of an Authorised Person.

**2.5 Security:** Processor shall implement appropriate technical and organisational measures to protect the Data from (i) accidental or unlawful destruction, and (ii) loss, unauthorized alteration, unauthorised disclosure of, or unauthorized access to the Data (a "Security Incident"). At a minimum, such measures shall include the security measures identified in Appendix 2 to Annex A.

**2.6 Subcontracting:** Processor shall not subcontract any processing of the Data to a third party sub-Processor without the prior written consent of Client. Notwithstanding this,

Client consents to Processor engaging third party sub-Processors, including Certified Partners of Processor, to process the Data provided that: (i) Processor will provide to Client an up-to-date list of its then-current sub-Processors upon request; (ii) Processor provides at least thirty (30) days' prior written notice of the addition or removal of any sub-Processor (including the categories of Data processed, details of the processing it performs or will perform, and the location of such processing). Processor's list of technical sub-Processors is maintained online and may be found here: <https://www.predictiveindex.com/subprocessors>; and Processor's list of service-related sub-Processors will be provided and maintained in an addendum to this Agreement. If, within thirty (30) days of Processor's notice to Client under clause (i) or (ii) of the preceding sentence ("Processor Notice"), Client notifies Processor of its refusal to consent to Processor's appointment of a third party sub-Processor on reasonable grounds relating to the protection of the Data, then either Processor will not appoint the sub-Processor or Client may elect to terminate this Agreement (and any other agreement between the Parties relating to the provision of services by Processor to Client) without penalty; provided that such termination right must be exercised within sixty (60) days of the date of the Processor Notice. In all cases, Processor shall impose the data protection terms on any sub-Processor it appoints that at a minimum meets the requirements provided for by this Agreement and Processor shall remain fully liable for any breach of this Agreement that is caused by an act, error or omission of its sub-Processor.

**2.7 Cooperation and individuals' rights:** To the extent permitted by Applicable Law, Processor shall provide reasonable and timely assistance to Client to enable Client to respond to: (i) any request from an individual to exercise any of its rights under Applicable Data Protection Law; and (ii) any other correspondence, enquiry or complaint received from an individual, regulator, court or other third party in connection with the processing of the Data. In the event that any such communication is made directly to Processor, Processor shall instruct such individual to contact Client directly.

**2.8 Data Protection Impact Assessment:** If Processor believes or becomes aware that its processing of the Data is likely to result in a high risk to the data protection rights and freedoms of individuals, it shall promptly inform Client of the same. Processor shall provide Client with all such reasonable and timely assistance as Client may require in order to conduct a data protection impact assessment and, if necessary, consult with its relevant data protection authority.

**2.9 Security incidents:** Upon becoming aware of a Security Incident, Processor shall inform Client without undue delay (and, in any event, within 32 hours) and shall provide such timely information and cooperation as Client may require in order for Client to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Law and relevant contractual obligations owed by Client to its subscribers. Processor shall cooperate with Client in taking all appropriate measures and actions as are necessary to remedy or mitigate the effects of the Security Incident, shall manage and modify its systems to remedy or mitigate such Security Incident and the likelihood

of future similar Security Incidents, and shall keep Client informed of all developments in connection with the Security Incident. Processor shall not notify any third parties of a Security Incident affecting the Data unless and to the extent that: (a) Client has agreed to such notification, and/or (b) notification is required to be made by Processor under Applicable Data Protection Laws. For the avoidance of doubt, Processor shall have the right to comply with the terms of its contracts with other customers with respect to their data.

**2.10 Deletion or return of Data:** Upon termination or expiry of the Agreement, Processor shall (at Client's request) destroy all Data (including all copies of the Data) in its possession or control (including any Data subcontracted to a third party for processing); provided, however, that customer data (including Data) may be retained on backup for a period of up to two (2) years for legal and compliance purposes. Notwithstanding the foregoing, Processor shall not reduce the security measures at any time until such Data is permanently deleted.

**2.11 Audit:** Processor shall permit Client (or its appointed third party auditors) to audit Processor's compliance with this Agreement, and shall make available to Client all information, systems and staff necessary for Client (or its third party auditors) to conduct such audit. Processor acknowledges that Client (or its third party auditors) may enter its premises for the purposes of conducting this audit, provided that Client gives it reasonable prior notice of its intention to audit, conducts its audit during normal business hours, and takes all reasonable measures to prevent unnecessary disruption to Processor's operations. Client will not exercise its audit rights more than once in any twelve (12) calendar month period, except (i) if and when required by instruction of a competent data protection authority; or (ii) Client believes a further audit is necessary due to a Security

Incident suffered by Processor. Processor shall also respond to any written audit questions submitted to it by Client. Notwithstanding anything else, Client understands and agrees that Processor operates a multi-tenant environment and Processor shall not be required to conduct, or permit Client or its auditors to conduct, any activities that could impair the security or confidentiality of the information of any of Processor's other customers.

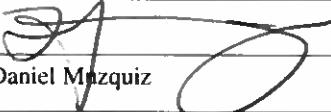
**2.12 Indemnity:** Processor (the "Indemnifying Party") shall defend and fully indemnify Client from and against all loss, harm, cost (including reasonable attorney's fees), fines, expense, and liability that Client may suffer or incur arising as a result of Processor's breach or non-compliance with this Agreement. The foregoing shall be subject to the indemnification procedures set forth in the PI Client Agreement.

**2.13 General cooperation to remediate:** In the event that Applicable Data Protection Law, or a data protection authority or regulator, provides that the transfer or processing of Personal Data under this Agreement is no longer lawful or otherwise permitted, then the Parties shall agree to remediate the processing (by amendment to this Agreement or otherwise) to the extent practical in order to meet the necessary standards or requirements. If Processor is unable to remediate the processing, then Client will be entitled to terminate the Agreement (and any other agreement between the Parties relating to the provision of services by Processor to Client) without penalty.

### 3. TERM

**3.1** The obligations placed upon the Processor under this Agreement shall survive so long as Processor and/or its sub-Processors process Personal Data on behalf of Client.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement by their duly authorized officers or representatives as of the Effective Date:

PREDICTIVE INDEX, LLC (DATA IMPORTER):		Client (DATA EXPORTER)	
BY		BY	
NAME	Daniel Muzquiz	NAME	
TITLE	President	TITLE	
ADDRESS	Westwood, Massachusetts, USA	ADDRESS	
DATE	5/2/2019	DATE	

[ANNEX A]

**Standard Contractual Clauses**

**Name of the data exporting organization:**

Each of the Client Group Companies listed in Appendix 3 (collectively referred to herein as "Client")

(each a. data exporter)

And

**Name of the data importing organization: Predictive Index, LLC**

(the data importer)

each a "party"; together "the parties"

**Recitals:**

- (A) The data exporter hires employees to work at its various facilities and utilizes various human resources tools to assess individuals.
- (B) In this capacity, the data exporter processes personal data as a controller (for example, the personal data of data exporter's employees who are residents in the European Economic Area.).
- (C) The data exporter wishes to appoint the data importer to provide data processing services on its behalf. The data that the data exporter will transfer to the data importer will include personal data for which the data exporter is the controller as described above.
- (D) The data importer shall process all personal data transferred to it in accordance with the Standard Contractual Clauses (hereinafter referred to as the, "Clauses"), regardless of whether the data exporter or a third party is the controller of that personal data.
- (F) The data exporter wishes to ensure an adequate level of protection for the personal data processed by the data importer outside of the European Economic Area. Accordingly, the parties have agreed on the following 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.

**1. Definitions:**

For the purposes of the Clauses:

'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in the applicable data protection law on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

'the data exporter' means the controller who transfers the personal data. This shall include each of the Client entities identified in Appendix 3 to these Clauses who, when transferring personal data to the data importer on behalf of a third party controller, will act in a manner consistent with the instructions of the controller of the personal data.

'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 the applicable data protection laws.

'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.

**'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 European Member State (the "Member State") in which the data exporter is established. The term applicable data protection law shall include EU Regulation 2016/679 (the General Data Protection Regulation) with effect from 25 May 2018 (and any applicable national laws made under it).

**'technical and organizational 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.

## **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.

## **3. Third-party beneficiary clause**

- 3.1** 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.
- 3.2** 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.
- 3.3** 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.
- 3.4** 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.

## **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 organizational 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 the applicable data protection law;
- (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 sub-processing 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).

## 5. Obligations of the data importer

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 organizational 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 subprocessинг, 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; and
- (j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

## **6. Liability**

- 6.1 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.
- 6.2 If a data subject is not able to bring a claim for compensation in accordance with paragraph 6.1 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 or by operation of law, in which case the data subject can enforce its rights against such entity.
- 6.3 The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.
- 6.4 If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 6.1 and 6.2, 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.

## **7. Mediation and jurisdiction**

- 7.1 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 and as specified in Appendix 4:
  - (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority; or
  - (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

- 7.2 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.

## **8. Cooperation with supervisory authorities**

- 8.1 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.
- 8.2 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.
- 8.3 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 8.2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

## **9. Governing Law**

The Clauses shall be governed by the law of the Member State in which the relevant controller of the personal data in question is established as further specified in Appendix 4.

## **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.

## **11. Subprocessing**

11.1 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. 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.

11.2 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.

11.3 The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 11.1 shall be governed by the law of the Member State in which the relevant controller of the personal data in question is established.

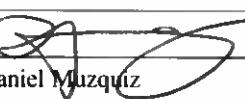
11.4 The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

## **12. Obligation after the termination of personal data processing services**

12.1 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.

12.2 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 12.1.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement by their duly authorized officers or representatives as of the date last signed below (the "Effective Date"):

PREDICTIVE INDEX, LLC (DATA IMPORTER)		Client (DATA EXPORTER)	
BY		BY	
NAME	Daniel Muzquiz	NAME	
TITLE	President	TITLE	
ADDRESS	Westwood, Massachusetts, USA	ADDRESS	
DATE	5/2/2019	DATE	

## **Appendix 1 to the Standard Contractual Clauses**

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

### **Data exporter**

Each data exporter is either a member of the Client group of companies whose ultimate parent company is Client, Inc. The Client group of companies provides and operates the Service.

Each data exporter wishes to appoint the data importer to provide it with data processing services. The role of the data importer, the nature of the data processing services it will provide, the categories of data that it will process, and the protections it will apply to protect those data are set out in the Appendices 1 and 2 to these Clauses.

### **Data importer**

The data importer is (please specify briefly activities relevant to the transfer):

A service provider which processes Personal Data of data exporter's personnel and/or end-users upon the instruction of the data exporter in accordance with the terms of the agreement between Client and data importer relating to the provision of services by data importer to Client.

### **Data subjects**

The personal data transferred concern the following categories of data subjects (please specify):

Data exporter may transfer Personal Data to data importer, the extent of which is determined and controlled by data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and Processors of data exporter (who are natural persons);
- Employees or contact persons of data exporter's prospects, customers, business partners and Processors; and
- Employees, agents, advisors, freelancers of data exporter (who are natural persons).

### **Categories of data**

The personal data transferred concern the following categories of data (please specify):

Data exporter may transfer Personal Data to data importer, the extent of which is determined and controlled by data exporter in its sole discretion the following categories of Personal Data:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- Employee ID data
- Home address, personal phone numbers, resumes)
- Location data

### **Special categories of data (if appropriate)**

The personal data transferred concern the following special categories of data (please specify):

None.

**Processing operations**

The personal data transferred will be subject to the following basic processing activities (please specify):

The objective of Processing of Personal Data by data importer is the performance of the data importer's services pursuant to the agreement between Client and data importer relating to the provision of services by data importer to Client.

IN WITNESS WHEREOF, the parties hereto have executed this Appendix by their duly authorized officers or representatives as of the date last signed below (the "Effective Date"):

<b>PREDICTIVE INDEX, LLC. (DATA IMPORTER)</b>		<b>Client (DATA EXPORTER)</b>	
<b>BY</b>		<b>BY</b>	
<b>NAME</b>	Daniel Muzquiz	<b>NAME</b>	
<b>TITLE</b>	President	<b>TITLE</b>	
<b>ADDRESS</b>	Westwood, Massachusetts, USA	<b>ADDRESS</b>	
<b>DATE</b>	5/2/2019	<b>DATE</b>	

## Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

**Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):**

**1. Physical Access Controls:** data importer shall take reasonable measures to prevent physical access, such as security personnel and secured buildings and factory premises, to prevent unauthorized persons from gaining access to personal data.

**2. System Access Controls:** data importer shall take reasonable measures to prevent personal data from being used without authorization. These controls shall vary based on the nature of the processing undertaken and may include, among other controls, authentication via passwords and/or two-factor authentication, documented authorization processes, documented change management processes and/or, logging of access on several levels.

**3. Data Access Controls:** data importer shall take reasonable measures to provide that personal data is accessible and manageable only by properly authorized staff, direct database query access is restricted and application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the personal data to which they have privilege of access; and, that personal data cannot be read, copied, modified or removed without authorization in the course of processing.

In addition to the access control rules set forth in Sections 1-

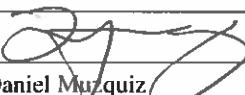
3 above, data importer implements an access policy under which access to its system environment, to personal data and other data by authorized personnel only.

**4. Transmission Controls:** data importer shall take reasonable measures to ensure that it is possible to check and establish to which entities the transfer of personal data by means of data transmission facilities is envisaged so personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport.

**5. Input Controls:** data importer shall take reasonable measures to provide that it is possible to check and establish whether and by whom personal data has been entered into data processing systems, modified or removed. Data importer shall take reasonable measures to ensure that (i) the personal data source is under the control of data exporter; and (ii) personal data integrated into data importer's systems is managed by secured file transfer from the data importer and data subject.

**6. Data Backup:** data importer shall ensure that back-ups are taken on a regular basis, are secured, and encrypted when storing personal data to protect against accidental destruction or loss when hosted by data importer.

IN WITNESS WHEREOF, the parties hereto have executed this Appendix by their duly authorized officers or representatives as of the date last signed below (the "Effective Date"):

PREDICTIVE INDEX, LLC (DATA IMPORTER)		Client (DATA EXPORTER)	
BY		BY	
NAME	Daniel Muzquiz	NAME	
TITLE	President	TITLE	
ADDRESS	Westwood, Massachusetts, USA	ADDRESS	
DATE	5/2/2019	DATE	

**Appendix 3 to the Standard Contractual Clauses**

**List of Client Group Companies**

Name of Entity	Registered Address	Registration Number
----------------	--------------------	---------------------