MRG DATA PROCESSING AGREEMENT

Updated October 27, 2023

The Data Processing Agreement ("DPA"), which includes Standard Contractual Clauses ("SCCs") adopted by the European Commission in accordance with the General Data Protection Regulation (REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 (the "GDPR") forms part of the Master Service Agreement or other written or electronic agreement between Management Research Group, Inc. ("Importer", "MRG") and _____ ("Exporter" / "Customer") for the purchase of products or services from the Importer's Assessment Web Applications ("Services") which includes Quest and/or Momentum, to reflect the parties' agreement with regard to the Processing of Personal Data, in compliance with all applicable laws, enactments, regulations, orders, standards, and other similar instruments that apply to its data processing operations.

1) THIS DPA INCLUDES:

a) Standard Contractual Clauses, attached hereto as EXHIBIT 1, and includes the following subparts:
b) APPENDIX Annex 1 to the SCCs, includes specifics on the Personal Data transferred by the data exporter to the data importer.
c) APPENDIX Annex 2 to the SCCs, includes a description of the technical and organizational safeguards implemented by the data importer as referenced.
d) A current list of Sub-processors, attached hereto as Annex 3.

2) HOW TO EXECUTE THIS DPA:

The DPA has been pre-signed by Management Research Group, Inc. as the Data Importer. To complete the DPA, the Customer must:

a) Add your business name to the blank space provided in the first paragraph of this document.
b) Complete the information in the signature block of this DPA and have an authorized representative sign on page 5.
c) Complete the information as the data exporter on pages 7 and 17.
d) Complete the information in the signature block and sign on pages 17 and 21.
e) Submit the completed and signed DPA to MRG at privacy@mrg.com. Upon receipt of the validly completed DPA at this email address, the DPA will be reviewed by MRG. Upon review and acceptance by MRG, this document will become legally binding.

3) HOW THE DPA APPLIES:

a) If the entity signing the DPA is a party to the Agreement, the DPA is an addendum to and forms part of the Agreement.
b) If the entity signing the DPA has executed a Purchase Order or Engagement Letter with MRG pursuant to the Agreement but is not itself a party to the Agreement, the DPA forms an addendum to that Purchase Order or Engagement Letter and applicable renewal Forms, and the entity that is a party to such Order Form is a party to the DPA.

c) If the entity signing the DPA is not a party to a Purchase Order or Engagement Letter nor a Master Service Agreement directly with MRG, but instead a customer indirectly via an authorized certified network partner of MRG, the DPA is stand-alone and governs only the importer/exporter relationship between MRG and that entity, and creates no other contractual obligations on the part of MRG.
d) The DPA shall not replace any comparable or additional rights relating to the Processing of Customer Data contained in any existing Agreement.

DPA DEFINITIONS

"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 preempt, 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.

"GDPR" means the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 as retained by the UK on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

"Personal Data" means any information relating to an identified or identifiable natural person (a "Data Subject"); 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.

"Process" or "Processing" means any operation or set of operations that is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Data Processor" or "Processor" means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

"Exporter" or "Data Exporter" 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.

"Importer" or "Data Importer" means a natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of the Exporter, in this case, MRG.

"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.

“Sub-processor” means any Data Processor engaged by MRG.

For the purposes of the Agreement, the terms '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.

DPA TERMS

1) **Provisions of the Service.** In the course of providing the Services to Customer, MRG may be required to process Personal Data on behalf of Customer. MRG and Customer each agree to comply with the following provisions with respect to any Personal Data submitted by or for Customer to the Services or collected and processed by or for the Customer through use of the Services.

2) **The Parties' Roles.** Each party acknowledges and agrees that with regard to the Processing of Personal Data, Customer is the Data Exporter, MRG is the Data Importer, and that MRG will have and maintain the right to select and engage Sub-processors upon notice to but without additional approval by Customer, for the Processing of Personal Data pursuant to the requirements of this DPA.

3) **Customer Responsibilities.** Customer shall, in its use of the Services, agree to Process Personal Data in compliance with all applicable laws, enactments, regulations, orders, standards, and other similar instruments that apply to its Processing operations. For the avoidance of doubt, Customer, as Data Controller, will ensure that any instructions provided to MRG for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Importer acquires the Personal Data.

4) **Processing Purposes.** MRG shall only Process Personal Data on behalf of and in accordance with Customer's instructions and shall treat Personal Data as confidential information. Customer instructs MRG to Process Personal Data for the following purposes: (i) Processing in accordance with the Agreement and applicable orders; (ii) Processing initiated by Customer's authorized users in their use of the Services; and (iii) Processing to comply with other reasonable and lawful instructions provided by Customer (e.g., via a support ticket) where such instructions are consistent with the terms of the Agreement.

5) **Scope of Processing.** The subject matter of the Processing of Personal Data by MRG is the performance of the Service pursuant to the Agreement. The nature and purpose of the Processing, the types of Personal Data, and categories of Data Subjects Processed under this DPA are specified in APPENDIX Annex 1.

6) **Data Subject Requests.** MRG will provide reasonable assistance, including via appropriate technical and organizational measures and taking into account the nature of the Processing, to enable Customer to respond to any request from Data Subjects seeking to exercise their rights under the Data Protection Law with respect to Personal Data (including access, rectification, restriction, deletion, or portability of

Personal Data, as applicable), to the extent permitted by the law. If such a request is made directly to MRG, MRG will promptly inform Customer and will advise Data Subjects to submit their request to Customer. Customer shall be solely responsible for responding to any Data Subjects' requests.

7) **Training.** MRG shall ensure that its relevant employees, agents, Sub-processors, and contractors receive appropriate training regarding their responsibilities and obligations with respect to the processing, protection, and confidentiality of Personal Data.

8) **Data Protection Officer.** Effective from 25 May 2018, MRG has appointed a Data Protection Officer and they may be reached at privacy@mrg.com or by contacting customer service.

9) **Sub-processors**. Customer acknowledges and agrees that MRG may engage third-party Sub-processors in connection with the provision of the Services. Any such Sub-processors will be permitted to obtain Personal Data only to deliver the services MRG has retained them to provide and are prohibited from using Personal Data for any other purpose. MRG agrees that any agreement with a Sub-processor will include materially similar data protection obligations as set out in this DPA. For these purposes, Customer consents to the engagement as sub-Processors of the third parties listed in Annex 3.

   For the avoidance of doubt, the above authorization constitutes Customer's prior written consent to the sub-Processing by MRG for purposes of Clause 11 of the Standard Contractual Clauses. MRG shall be liable for the acts and omissions of its Sub-processors to the same extent MRG would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

10) **Security.** MRG shall maintain administrative, physical, and technical safeguards for the protection of the availability, confidentiality, and integrity of Personal Data, known as Technical and Organizational measures.

11) **Personal Data Breach Notification.** If MRG becomes aware of any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to any Personal Data transmitted, stored, or otherwise processed, MRG will notify all impacted parties as soon as possible once the security breach has been determined. MRG also commits to notifying applicable regulatory bodies and or law enforcement as required by law without undue delay, and within 72 hours, after confirmation of a breach.

12) **Retention of Personal Data.** Data processed through our Assessment websites will be retained by MRG for as long as the Controller or Processor is a client of MRG, or until the data is requested to be deleted by the Data Subject, or until the data is no longer necessary to provide the requested services. Anonymized data may be aggregated for MRG's research, norming, and comparison purposes. However, MRG will always respect Data Subject's request for deletion of Personal Data, subject to limitations of applicable laws and regulations.

13) **Ex-EEA Transfer of Data.** In accordance with GDPR Article 45(3), MRG operates within the European Commission's adequacy decision on July 10, 2023, and has adopted the EU-U.S Data Privacy

Framework, UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework, collectives referred to as the (“DPF”). MRG certifies compliance with the DPF, including strict compliance with approved US and EU redress mechanisms for data requested by US intelligence agencies or through National Security Letters. Where appropriate and upon request, we continue to use SCCs to govern data transfer safety from the UK, EU, and Switzerland to the United States. MRG has proven and demonstrated commitment to safe data transfer principles, including the use of European EU data protection authorities (DPAs), the UK’s Information Commissioner’s Office (ICO), and the Swiss Federal Data Protection and Information Commissioner (FDPIC), and complies with the advice given by such authorities with regard to all data transferred from the EU, UK, and Switzerland.

14) **Parties to this DPA**. Nothing in this DPA shall confer any benefits or rights on any person or entity other than the parties to this DPA.

ACCEPTED AND AGREED TO:
Management Research Group, Inc.

Name:Jason J. Sgro
Title: Data Protection Officer
Date: 10/27/2023 (“Signed Date”)

Name: Lida Hutchings
Title: Head of Finance & Talent
(Corporate Officer)
Date: 10/27/2023

AND

Customer Authorized Signer.
[PLEASE SIGN AND COMPLETE]

_____

Name: _____
Title: _____
Date: _____

EXHIBIT 1

Standard Contractual Clauses (processor to controller P2C)

With respect to Personal Data transferred from the European Economic Area, the New SCCs will apply and form part of this Agreement. For the purposes of the new SCCs, they shall be deemed completed as follows:

1) For the purposes of this DPA and SCCs, Customer acts as a Data Controller, and MRG acts as Customer's processor with respect to the Personal Data subject to the New EU SCCs, and Module 4 applies.

2) For the purposes of these SCCs, Customer will be the Data Exporter and MRG will be the Data Importer.

3) The relevant provisions in the new and old SCCs are incorporated by reference and form an integral part of this DPA.

4) The optional clause 7 docking clause does not apply.

5) Under Clause 9 (Use of sub-processors), MRG selects Option 2 (General written authorization). The initial list of sub-processors is set forth in Annex 3, and MRG shall provide notice of any changes to that list through the addition or replacement of Sub-processors.

6) Clause 13 does not apply to P2C Clauses.

7) Under Clause 17, MRG chooses Option 1 (the law of an EU Member State that allows for third-party beneficiary rights).

8) Under Clause 18 (Choice of forum and jurisdiction), the parties select the jurisdiction where the Data Exporter is established.

9) Annex 1 of the New EU SCCs is set forth in this Agreement.

10) Annex 2 does not apply to P2C clauses, but we have voluntarily included it for transparency.

11) Annex 3 does not apply to P2C clauses, but we have included sub-processor information for transparency.

12) The "exporter" is the Customer and the exporter's contact information is set forth below. The "importer" is MRG and MRG's contact information is set forth below.

13) The "illustrative indemnification clause" labeled "optional" is not applicable.

14) To provide additional safeguards, the obligations in Module 2 of Section III of the New EU SCCs (Local Laws and Obligations in Case of Access by Public Authorities) shall form part of this DPA with respect

to Personal Data subject to the UK Data Protection Act 2018, regardless of whether the rest of the New EU SCCs apply to any Personal Data.

[PLEASE COMPLETE]

Name of the data exporting organization: _____
(“Customer”) Address:
_____
Tel.: _____; fax: _____; e-mail: _____
Date:_____ (“Effective Date”)
Other information needed to identify the organization:

(the data exporter)

And

Management Research Group, Inc. (“MRG”)
Address: 14 York Street, Suite 301, Portland, Maine 04101
Tel.: +1-207-775-2173 e-mail: privacy@mrg.com
MRG

(the data importer)

each a “party”; together “the parties”,

HAVE AGREED on the following SCCs 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 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;

(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 their behalf after the transfer in accordance with their 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 sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor 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, including but not limited to the GDPR, 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 organizational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure, or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

(g) “clauses” shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

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 Regulations) (1) for the transfer of personal data to a third country.

(b) The Parties:

> (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”),
>
> and
>
> (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A, (hereinafter each “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 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 - Module One: Clause 8.5(e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1(b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two, and Three: Clause 18(a) and (b); Module Four: Clause 18 (b) Paragraph (a) is without prejudice to the 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

Docking Clause. Optional Docking Clause does not apply.

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 organizational 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 acting as its controller.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data exporter shall refrain from any action that would prevent the data importer from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) 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.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organizational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall

take due account of state of the art, the costs of implementation, the nature of the personal data, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data importer under these Clauses, the data importer shall notify the data exporter without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9
Use of sub-processors

GENERAL WRITTEN AUTHORIZATION The data importer has the data exporter's general authorization 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 45 days in advance.

Clause 10
Data Subject Rights

The Parties shall assist each other in responding to inquiries and requests made by data subjects under the local law applicable to the data exporter or, for data processing by the data importer, under Regulation (EU) 2016/679.

Clause 11
Redress

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 authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

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) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party 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 under Regulation (EU) 2016/679.

(c) 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.

(d) The Parties agree that if one Party is held liable under paragraph (c), 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.

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

Clause 13

Not Applicable (P2C – Module four)

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

Clause 14

Local laws and practices affecting compliance with the Clauses.
Transfer processor to controller (where the EU processor combines the personal data received from the third country controller with personal data collected by the processor in the EU).

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 authorizing 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:
   (1) 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;

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

(3) any relevant contractual, technical, or organizational 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 organizational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three: if appropriate in consultation with the controller]. 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 [for Module Three: the controller or] 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, Clauses 16(d) and (e) shall apply.

Clause 15 – OBLIGATIONS OF THE DATA IMPORTER

Transfer processor to controller (where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU).

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 minimization
(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 collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. 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 a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of the nation in which the data exporter is headquartered.

Clause 18

Choice of forum and jurisdiction. Any dispute arising from these Clauses shall be resolved in the jurisdiction of the data exporter.

APPENDIX 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.

ANNEX 1

A. LIST OF PARTIES

Data exporter (controller)
[PLEASE COMPLETE]

Name (written out in full): _____
Contact Person Name, position, contact details: _____
Address: _____

Please briefly specify your activities relevant to the data transferred under these Clauses:
_____ is _____

Data importer (processor)

Name: Management Research Group Inc. (MRG)
Contact Person Name (written out in full): Jason J. Sgro
Position: Data Privacy Officer
Address: 33 Jewell Ct. Portsmouth, NH 03801

Activities relevant to the data transferred under these Clauses:

MRG is a global provider of assessments and consulting solutions which processes personal data and participant responses upon the instruction of the data exporter in accordance with the terms of the Service Agreement.

B. DESCRIPTION OF TRANSFER

Nature and Purpose
MRG will process Personal Data as necessary to provide the Services under the Agreement. MRG does not sell customer data and does not share such end users' information with third parties for compensation or for those third parties' own business interests.

Data Subjects
The personal data transferred concern the following categories of data subjects:
Data subjects may include employees, contractors, business partners, potential employees, prospects and customers of the data exporter, vendors and subcontractors, or other individuals utilizing the services.

Categories of data
The personal data transferred concerns the following categories of data (please specify):
The data exporter may submit Personal Data, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following: name, email, title, company identification, responses to assessment items, results garnered through the process.

Special categories of data (if appropriate)
The personal data transferred concerns the following special categories of data (please specify): Data subjects may provide ethnicity information, age, and gender on an optional basis only. The frequency of the transfer Customer Personal Data may be transferred on a continuous basis until it is deleted in accordance with the terms of the Data Processing Agreement.

ANNEX 2

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4 and 5:

MRG has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect the data against accidental loss, destruction, alteration, unauthorized disclosure or access, or unlawful destruction.

1) **Quest Assessment Management System Security, Maintenance & Monitoring**
   a) **Quest Data.** Quest requires the following data to be able to complete an assessment: First Name, Last Name and Email Address.
   b) **Assessment Responses.** Responses are stored in an anonymized format in our databases and used for internal MRG Research purposes only. MRG does not share or sell any assessment response data.

c) **Application Security.** Quest is protected by application-level security. It requires Username/Password authentication in order to gain access. The site is fully encrypted using https protocols.
d) **Password Policy.** The security settings enforce NIST 800-63B Authenticator Level 1 standards for password complexity and identity management.
e) **Account Lockout Policy.** The security settings enforce account lockout threshold at 3 invalid login attempts for duration of 30 minutes and requires subsequent re-authentication.
f) **Application Monitoring.** Quest is monitored by HTTP requests every 30 seconds. Both successful and unsuccessful requests are logged for up-time reporting purposes. MRG staff are notified immediately if a request is not successful.
g) **Segregation of Live Data.** MRG's Development and Production environments are run on different virtual servers. No Development occurs in the production environment. Access to the production servers and client data is systematically restricted using strict adherence to roles and client-based permissions.
h) **Software Upgrades and New Releases.** Software fixes are released on a scheduled basis. All enhancements, bugs and other changes are tracked using issue tracking software. All enhancements to existing platforms and products are subjected to a staging process where functionality, data security, and impact on related systems are tested. MRG conducts structured tests from the programming and end-user requirements perspectives, prior to any release.
i) **Virtualization**. All production servers are deployed using virtualization. This platform is built with high availability allowing for automated system recovery for Host specific disasters. In the event of a major full site disaster, MRG's highly portable virtual infrastructure lends itself to quick off-site recovery in our vendor's data center.
j) **Data Storage Locations.** MRG utilizes cloud-based servers managed in Reston, VA, United States of America. All data entered into the Services will be stored in this location.
k) **Personnel Security.** MRG personnel and authorized vendors are required to conduct themselves in a manner consistent with the MRG's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards.

DATA EXPORTER *[PLEASE SIGN]*

Name: _____

Authorized Signature: _____

DATA IMPORTER
Name: Management Research Group, Inc.
Authorized Signature:

Jason J. Sgro
Data Protection Officer

ANNEX 3

LIST OF SUB-PROCESSORS

- iLand, *located within the states of Maine and Virginia, within the United States of America. iLand provides the cloud hosting services for MRG Technology.*

- Systems Engineering, *located in the states of Maine, within the United States of America. Systems Engineering performs IT maintenance services and disaster recovery services for MRG.*

- SalesForce.com, Inc, *is a global SaaS solution utilized for the sales, marketing, and user administration.*

- HubSpot *is a global SaaS solution utilized for marketing automation and corporate brand administration.*