MRG DATA PROCESSING ADDENDUM
(GDPR and EU Standard Contractual Clauses)

Where applicable, this Data Processing Agreement ("DPA"), that includes Standard Contractual Clauses ("SCCs") adopted by the European Commission, forms part of the Master Service Agreement or other written or electronic agreement between Management Research Group, Inc. ("Importer", "MRG") and Customer ("Exporter", "Customer") for the purchase of products or services from the Importer's Assessment websites (Quest and/or Momentum) to reflect the parties' agreement with regard to the Processing of Customer Data, including Personal Data, in accordance with the requirements of applicable Data Protection Laws and Regulations.

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.

HOW TO EXECUTE THIS DPA:

1. The DPA has been pre-signed by Management Research Group, Inc. as the data importer.
2. To complete the DPA, Exporter must:
   a) Complete the information in the signature block of this DPA and have an authorized representative sign on page 4.
   b) Complete the information as the data exporter on page(s) 5 and 12.
   c) Complete the information in the signature block and sign on page(s) 11, 13 and 16.
3. 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 become legally binding.

HOW THE DPA APPLIES:

a) If the entity signing the DPA is a party to the Agreement, the DPA are an addendum to and form 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 are an addendum to that Purchase Order or Engagement Letter and applicable renewal Forms, and the entity that is party to such Order Form is 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 stand alone and govern only the importer / exporter relationship between MRG and that entity, and create 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 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. The terms "process", "processes" and "processed" will be construed accordingly. **"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.

"Data Subject" means the individual to whom Personal Data relates.

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

"Personal Data" means any information relating to an identified or identifiable individual where such information is contained within Customer 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.

"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.

"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.

"Sub-processor" means any Data Processor engaged by MRG.

DPA TERMS

1. Provisions of the Service. In the course of providing the Assessment websites (Quest and/or Momentum) to Customer, MRG may 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 Assessment websites) or collected and processed by or for the Customer through the Assessment websites.

2. The Parties' Roles. The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Data Exporter, MRG is the Data Importer and that MRG will engage sub-processors pursuant to the requirements of this DPA.

3. Customer Responsibilities. Customer shall, in its use of Assessment website or receipt of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Customer will ensure that its instructions 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 acquired 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 Users in their use of the Assessment websites; and (iii) Processing to comply with other reasonable 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 Processing of Personal Data by MRG is the performance of the Service pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Appendix 1 to this DPA.

6. Data Subject Requests. MRG will provide reasonable assistance, including by 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 request is made directly to MRG, MRG will promptly inform Customer and will advise Data Subjects to submit their request to the Customer. Customer shall be solely responsible for responding to any Data Subjects' requests.

7. Training. MRG shall ensure that its relevant employees, agents 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 shall have appointed, or shall appoint, a data protection officer if and whereby such appointment is required by Data Protection Laws and Regulations. Any such appointed person may be reached at privacy@mrg.com.

9. Sub-processors. Customer acknowledges and agrees that MRG may engage third party Sub-processors in connection with 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 substantially the same 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 Exhibit 2. 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 protection of the security, confidentiality and integrity of Personal Data.

11. Security 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 as soon as possible once the security breach has been determined. MRG also commits to notifying all applicable DPAs (Data Protection Agencies) without undue delay, and within 72 hours if feasible, after becoming aware of a breach.

12. Retention of Personal Data. Data processed through our Assessment websites is retained indefinitely. However, MRG will always respect Exporter's request for deletion of Personal Data, subject to limitation to applicable laws and regulations.

13. Privacy Shield. MRG self-certified to and complies with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce, and MRG shall maintain its self-certification to and compliance with the Privacy Shield Principles with respect to the Processing of Personal Data that is transferred from the European Economic Area or Switzerland to the United States.

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.
Signature: _____	Signature: Heather R. Troidl
Name: _____	Name: Heather Troidl
Title: _____	Title: Data Protection Officer
Date: _____	

Management Research Group, Inc CORPORATE SEAL 1983 Maine

EXHIBIT 1 - 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

[PLEASE COMPLETE]
Name of the data exporting organisation:

Address:

Tel.: _____; fax: _____; e-mail: _____

Other information needed to identify the organization:

(the data exporter)

And

Name of the data importing organisation: Management Research Group, Inc. ("MRG")

Address: 14 York Street, Suite 301, Portland, Maine 04101

Tel.: +1-207-775-2173 e-mail: privacy@mrg.com

Other information needed to identify the organization:

MRG
(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 d ata','special categories of d ata','process/processing', 'controller', 'processor', 'd ata subj ect'*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];

[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.

(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 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 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.

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 sub processor 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 sub processor 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

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; and

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

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 sub processor 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 sub processor 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 sub processor 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 sub processor 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.

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, or as disclosed in Schedule 2. 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.

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.

On behalf of the data exporter: *[PLEASE COMPLETE AND SIGN]*

Name (written out in full): _____

Position: _____

Address: _____

Other information necessary in order for the contract to be binding (if any):

Signature:_____
(stamp of organization)

On behalf of the data importer:

Name (written out in full): Heather Troidl

Position: Data Privacy Officer

Address: 14 York Street, Suite 301, Portland, Maine 04101 USA

Other information necessary in order for the contract to be binding (if any):

Signature: Heather R. Troidl

Management Research Group, Inc CORPORATE SEAL 1983 Maine

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

[PLEASE COMPLETE]
The data exporter is (please specify briefly your activities relevant to the transfer):

_____ is _____

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

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.

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

Data subject may provide ethnicity information, age, and gender on an optional basis only.

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

Personal data may be processed for the following purposes: (a) to provide the services, including the detection, prevention and resolution of security and technical issues, back up of data, processing,

transmission, retrieval and access; (b) to respond to support requests; and (c) otherwise to fulfill the obligations of the purchase transaction between the parties.

DATA EXPORTER *[PLEASE SIGN]*

Name: _____

Authorised Signature: _____

DATA IMPORTER

Name: Management Research Group, Inc.

Authorised Signature: Heather R. Troidl

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 organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

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, or alteration; unauthorized disclosure or access; or unlawful destruction.

1. Quest Assessment Management System Security, Momentum System Maintenance & Monitoring

1.1 Quest & Momentum Data

Systems require the following data to be able to complete an assessment: First Name, Last Name and Email Address.

Assessment 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.

1.2 Application Security

Quest and Momentum are protected by application-level security. It requires Username/Password authentication in order to gain access. Both sites also are fully encrytped using https protocols.

1.3 Password Complexity Policy

The security settings enforce a minimum password length of 8 characters, including at least one numeric character and at least one UPPERCASE letter.

1.4 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.

1.5 Application Monitoring

Quest and Momentum are monitored by HTTP request every 30 seconds. Both successful and unsuccessful requests are logged for up-time reporting purposes. MRG staff is notified immediately if a request is not successful.

1.6 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.

1.7 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 is tested. MRG conducts structured tests from the programming and end-user requirements perspectives, prior to any release.

1.8 Virtualisation

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.

1.9 Data and Server Backup Strategy

MRG utilizes a two-tiered backup strategy utilizing local backups for the VM platform and SQL backups for the application data. The EVault Cloud storage system datacenter is used to store the data off-site with local access and secondary storage in diverse yet replicated datacenters that are SSAE-16 and SOC-2 compliant.

MRG backs up Quest data every 2 hours, as well as server backups daily to disk with multiple iterations stored off-site at the datacenter. A combination of weekly and monthly backups provides 9 iterations of data backup coverage at any point in time. Automated backups are monitored on a 24/7/365 basis by our vendor, Axis Business Solutions.

1.10 Quest Server Locations

MRG utilizes iLand's cloud-based servers managed by our strategic networking partner, Axis Business Solutions. MRG's physical Production and QA servers are hosted at iLand'sData Center in Reston, VA, USA which is SSAE-16 and SOC-2 compliant and replicated to redundant data centers in the United States.

2. Network Security and Monitoring

2.1 Network Vulnerability Management

All of MRG's local and remote servers, workstations and network devices are updated monthly with the latest appropriate Microsoft Security Patches and applicable Window Service Packs. If a critical update patch is published by Microsoft, it is reviewed for applicability for each server and workstation and installed outside the monthly maintenance schedule if deemed necessary.

All of MRG's local and remote servers and workstations run active anti-virus software. This is monitored on a 24/7/365 basis by our vendor, Axis Business Solutions, who confirms antivirus protection is current and functional and that scheduled virus definition updates are occurring.

2.2 Network Monitoring

Our network is monitored 24-hours a day, seven days a week by Axis Business Solutions. MRG's Business Technology System Administrators are notified upon failure of any device on the network.

3. Access and Site Control

3.1 Access Control and Privilege Management. Clients' administrators and end users must authenticate themselves via a central authentication system in order to use the Service. Each application checks credentials in order to allow the display of data to an authorized end user or authorized administrator.

3.2 Internal Data Access. MRG's internal data access process and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process Personal Data. MRG requires the use of unique user IDs and strong passwords to minimize the potential for unauthorized account use. The granting and modification of access rights is based on: the authorized personnel's job responsibilities, job duty requirements necessary to perform authorized tasks; and a need to know basis. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g. login to workstations), password policies that follow at least industry standard practices are implemented. These standards include password expiry, restrictions on password reuse and sufficient password strength.

4. Personnel Security

MRG personnel and authorized vendors are required to conduct themselves in a manner consistent with the Company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards.

Personnel acknowledge receipt of, and compliance with MRG's policies and non-disclosure agreement.

DATA EXPORTER *[PLEASE SIGN]*

Name: _____

Authorised Signature: _____

DATA IMPORTER

Name: Management Research Group, Inc.

Authorised Signature: Heather R. Troidl

EXHIBIT 2 - List of Sub-Processors

- iland
- Axis Business Solutions
- Carbonite, Inc. and its affiliates and subsidiaries (collectively "Carbonite") HubSpot, Inc.
    - Any other wholly-owned HubSpot, Inc. subsidiary organizations
- Salesforce, Inc.
    - Any other wholly-owned Salesforce, Inc. subsidiary organizations