***BOSTON RESEARCH GROUP, INC.***
***INTERNATIONAL DATA PROTECTION POLICY***

(As submitted to the US Department of Commerce U.S.-EU Safe Harbor Framework
and last updated on December 1, 2013)

## 1. Purpose

This Policy defines requirements to ensure compliance with laws and regulations applicable to Boston Research Group ("BRG") collection, use, and transmission of Personal Data throughout the world.

## 2. Scope

BRG is committed to complying with the applicable data privacy and security requirements in the countries in which it and its partners (the "Company") operate. Because of differences across countries, the Company has developed a data protection policy which outlines processes and procedures intended to achieve compliance in countries were the Company conducts business.

This Policy applies to all BRG full and part time employees and all suppliers and vendors who receive Personal Data from BRG, have access to Personal Data collected or processed by BRG, or who provide information to BRG, regardless of geographic location.

BRG's compliance program is overseen by the Board of Directors of BRG. The Board of Directors will ensure that all employees, suppliers and third parties are informed of these data protection policies and any penalties which may be assessed for any violations. The Board of Directors will also update this Data Protection Policy from time to time as necessary to ensure compliance in handling Personal Data.

## 3. Notifications

BRG's Data Protection Policy requires that in every case that Personal Data is collected, accessed or transferred that a determination be made as to whether notification to a data protection authority is required and, if so, to make those notifications. The policy further requires that vendors, suppliers, and third parties who interchange Personal Data with BRG are compliant with proper notifications.

## 4. Data Protection Principles

Boston Research Group complies with the U.S.-EU Safe Harbor Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries. Boston Research Group has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement. To learn more about the Safe Harbor program, and to view Boston Research Group's certification, please visit http://www.export.gov/safeharbor/

BRG has adopted the following principles to govern its use, collection, and transmittal of Personal Data, except as specifically provided by this Policy or as required by applicable laws:

- Personal Data shall only be obtained, processed, and transferred fairly and lawfully as required by any jurisdiction in which these actions are taken.
- Personal Data shall be accurate, complete and current as appropriate to the purposes for which they are collected and/or processed.
- Personal Data shall not be collected or processed unless:
  - Data Subject has provided a valid, informed consent
  - Processing is necessary for the performance of a contract to which the Data Subject is a party
  - Processing is necessary for compliance with a BRG legal obligation
- Appropriate physical, technical, and procedural measures shall be taken to prevent unauthorized or unlawful collection, processing, transmittal of Personal Data; and to prevent accidental loss or damage to Personal Data.

## 5. Consents

BRG shall establish systems for the collection and documentation of Data Subject consents to the collection, processing, and/or transfer of Personal Data. To be valid, consent must be informed, expressed, and freely given. Further, consent must be revocable. All consents must be documented including the date, method, and content of the disclosures being made.

## 6. Transfers to Third Parties

BRG Data Protection policy requires that Personal Data meet the following requirements for transfer to third parties.

- Personal Data shall not be transferred to another entity, country or territory, unless reasonable and appropriate steps have been taken to maintain the required level of data protection.

- Personal Data may be communicated to third persons only for reasons consistent with the purposes for which the data were originally collected or other purposes authorized by law.
- All Sensitive Data transferred outside of the Company or across public communications networks shall be protected against unauthorized access.
- EU Personal Data shall not be transferred to a country or territory outside the European Economic Area unless the transfer is made to a country or territory recognized by the EU as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the processing of Personal Data, or is made in compliance with one of the mechanisms recognized by the EU as providing adequate protection when transfers are made to countries or territories lacking an adequate level of legal protection.
- The Company has selected participation in the U.S. Department of Commerce "Safe Harbor" system as its method of providing adequate protection for transfers of EU Personal Data to the United States.
- Personal Data may be transferred where any of the following apply:
    - The Data Subject has given consent to the proposed transfer
    - The transfer is necessary for the performance of a contract between the Data Subject and the Company, or the implementation of pre-contractual measures taken in response to the Data Subject's request
    - The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Company and a Third Party
    - The transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise, or defense of legal claims
    - The transfer is required by law
    - The transfer is necessary in order to protect the vital interests of the Data Subject; or
    - The transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest.

## 7. Disclosures at the Time of Data Collection

BRG's Data Protection Policy requires that appropriate disclosures will be made at the time a Data Subject is asked to give consent to the collection or processing of Personal Data, and whenever Personal Data are collected. Guidelines for appropriate disclosers are:

- Proper disclosure must be given to the Data Subject at the time of collection
- Technical or administrative means must be established documenting the fact that the Data Subject was given or already has the disclosure information

- The disclosures may be given orally, electronically, or in writing. If given orally, the person making the disclosures should use a suitable script or form as a record establishing the fact, date, content, and method of disclosure.

## 8. Data Subject Access

BRG's Data Protection Policy requires the observation of the following Data Subject rights:

- Data Subjects have the right of access, blockage, erasure, opposition, rectification, and, where appropriate or required by applicable law, a system for giving notice of inappropriate exposure of Personal Data.
- Data Subjects shall be entitled to obtain the following information about their own Personal Data upon a request made in compliance with reasonable policies and procedures established, and set forth in writing, by the Board of Directors:
    - Whether the Company has stored Personal Data concerning the Data Subject.
    - Whether any of the data are Sensitive Data.
    - The source(s) of the data, if known.
    - The recipients or categories of recipients to whom the data have been or may be transmitted.
    - The purposes of the collection, processing, use and storage of the data.
    - A hard copy of the data in an intelligible form.
- Such requests should be sent via email to brgrep at bostonresearchgroup.com (use "@" with no spaces to format email address) or by mailing requests to: Board of Directors, Boston Research Group, Inc, One Ash Street, Hopkinton, MA 01746.
- The Board of Directors may establish procedures to screen and deny abusively burdensome or repetitive requests by or on behalf of a Data Subject.

## 9. Data Quality Assurance

BRG's Data Protection Policy requires the following measures to assure data quality:

- Personal Data must be complete and accurate
- Any incorrect data must be corrected
- Any incorrect data that can not be corrected must be discarded
- Personal Data must be kept only for the period necessary for permitted uses

## 10. Proportionality

This Data Protection Policy will be applied in a reasonable manner with cost and effort proportionate to the importance of the proposed processing and the sensitivity of the data at issue.

## 11. Use of Third Party Data Processors.

BRG Data Protection Policy establishes the following requirements for third parties when processing or handling Personal Data:

- The Board of Directors will choose a Data Processor who provides sufficient security measures and takes reasonable steps to ensure compliance with those measures.
- As part of BRG's internal data auditing process, BRG shall conduct regular checks on processing by third party data processors, especially in respect of security measures.

## 12. Data Security

BRG's Data Protection Policy requires that the Board of Directors shall adopt physical, technical, and organizational measures to ensure the security of Personal Data, including the prevention of their alteration, loss, damage, unauthorized processing or access, having regard to the state of the art, the nature of the data, and the risks to which they are exposed by virtue of human action or the physical or natural environment. Adequate security measures should include all of the following:

- Entry Control: Prevention of unauthorized persons from gaining access to data processing systems in which Personal Data are processed.
- Admission Control: Prevention of data processing systems from being used by unauthorized persons.
- Access Control: Preventing persons entitled to use a data processing system from accessing data beyond their needs and authorizations. This includes preventing unauthorized reading, copying, modifying or removal during processing and use, or after storage.
- Disclosure Control: Ensuring that Personal Data in the course of electronic transmission during transport or during storage on a data carrier cannot be read, copied, modified or removed without authorization, and providing a mechanism for checking to establish who is authorized to receive, and who has received, the information.
- Input Control: Ensuring that it can be subsequently checked and established whether and by whom Personal Data have been entered into, modified on or removed from data processing systems.
- Job Control: Ensuring that in the case of commissioned processing of Personal Data, the data can be processed only in accordance with the instructions of the Data Controller.
- Availability Control: Ensuring that Personal Data are protected against undesired destruction or loss.
- Use Control: Ensuring that data collected for different purposes can and will be processed separately.
- Longevity Control: Ensuring that data are not kept longer than necessary, including by requiring that data transferred to third persons be returned or destroyed.

## 13. Dispute Resolution

Data Subjects with inquiries or complaints about the processing of their Personal Data should bring the matter to the attention of the Board of Directors in writing. Any disputes concerning the processing of the Personal Data of Data Subjects will be resolved through arbitration (JAMS; www.jamsadr.com). Such inquiries or complaints should be sent via email to brgrep at bostonresearchgroup.com (use "@" with no spaces to format email address) or by mailing requests to: Board of Directors, Boston Research Group, Inc, One Ash Street, Hopkinton, MA 01746.

If a matter in dispute relates to whether transfers of data from the European Economic Area to the United States have been done in compliance with the requirements of the U.S. Safe Harbor Provisions, then such disputes shall be brought to the attention of the Board of Directors which shall make an independent investigation and evaluation of the Data Subject's complaint. If the matter is not resolved to the Data Subject's satisfaction through this mechanism, the matter shall be resolved in accordance with the provisions of the Safe Harbor mechanism with enforcement by the U.S. Federal Trade Commission, as provided by the Safe Harbor provisions.

## 14. Training

BRG will provide training to teach, or re-emphasize privacy and security related procedures. These procedures should be set forth in written guidelines to employees and shall include at least the following:

- Each employee's duty to use and permit the use of Personal Data only by authorized persons and for authorized purposes.
- The Data Protection Principles set forth
- The contents of this Policy;

## 15. Limited Effect of Policy

This Policy shall not be interpreted or construed as giving any individual rights greater than those which such person would be entitled to under applicable law and other binding agreements.

## 16. Compliance Measurement

The Board of Directors shall implement a data protection compliance audit. BRG shall review annually its data collection, processing, and security practices. This annual review shall consist of at least the following:

- What Personal Data the business unit is collecting, or intends to collect,
- the purposes of the data collection and processing,
- any additional permitted purposes,
- the actual uses of the data,
- what disclosures have been made about the purposes of the collection and use of such data,
- the existence and scope of any Data Subject consents to such activities,
- any legal obligations regarding the collection and processing of such data, and
- the scope, sufficiency, and implementation status of security measures.

## 17. Implementation

This Data Protection Policy shall be available to employees and shall be made available to non-employees through posting to www.BostonResearchGroup.com/english/safeharbor.

This Policy is adopted as of October 30, 2009. The Board of Directors will develop a timeline and program for implementing this Policy. This Policy may be revised at any time.

## 18. Sponsor and Custodian

The Board of Directors is responsible for maintenance and accuracy of this Policy. Any questions regarding this Policy should be directed to the Board of Directors.
Any questions regarding the implementation of this Policy should be directed to the Board of Directors. Such questions should be sent via email to brgrep at bostonresearchgroup.com (use "@" with no spaces to format email address) or by mailing requests to: Board of Directors, Boston Research Group, Inc, One Ash Street, Hopkinton, MA 01746.

## 19. Severability

Whenever possible, each Section of this Policy shall be interpreted in a manner as to be valid under applicable law, but if any provision shall be held to be prohibited or invalid, such provision shall be ineffective only to the extent of such prohibition or invalidity, without invalidating the remainder of such provision or the other remaining provisions of the this Policy.