BRG Global Privacy and Data Protection Policy

I. Purpose

This *Global Privacy and Data Protection Policy* ("Policy") establishes Berkeley Research Group's (BRG) Privacy Program and the principles that govern when, why, and how BRG Processes Personal Data and complies with Applicable Laws.

II. Scope

This Policy applies to all activities conducted by BRG that involve the Processing of Personal Data by BRG and to any BRG Personnel involved in such activities. BRG affiliates, divisions, and teams may adopt policies and procedures that are stricter than this Policy, subject to review and approval by the Legal department and Privacy team. All BRG Personnel must comply with this Policy. Failure to do so will result in corrective action consistent with Human Resources (HR) policies and practices.

III. Definitions

- "Applicable Laws" means all laws applicable to BRG wherever it does business, including laws governing Data Protection, Data Security, and data breach notification.
- "Data Protection" means protecting the privacy, confidentiality, and rights of Data Subjects and their Personal Data by reasonable and appropriate technical and organizational measures.
- "Data Security" means technical, administrative, and physical measures used to protect the availability, integrity, and confidentiality of information, including Personal Data.
- "Data Subject" means a living person to whom Personal Data relates. Various laws use different terms for similar concepts, such as "Consumer," "Patient," or "Identified Individual." Data Subjects may include, for example, BRG employees, client employees, or individuals included in data sets.
- "Data Subject Request" (DSR) is a request made by a Data Subject or a Data Subject's authorized representative to exercise one or more privacy rights they may have under Applicable Laws.
- "Personal Data" means any information related to an identified or identifiable individual person.
- "Personnel" means any BRG employee, agent, contractor, or other third party subject to BRG policies.
- "Privacy team" means the BRG team responsible for establishing, operationalizing, monitoring, enforcing, and maintaining BRG's Privacy Program in consultation with BRG's Legal department and Trust Office.

- "**Process**" or "**Processing**" means any operation performed on Personal Data, which includes, for example, collecting, recording, organizing, storing, adapting, editing, altering, retrieving, consulting, transmitting, disseminating, archiving, deleting, or otherwise using Personal Data. Generally, anything you do to or with Personal Data, including merely viewing it, is Processing.

IV. Privacy and Data Protection Principles

The following Privacy and Data Protection Principles govern BRG's Processing of Personal Data. BRG will develop and maintain internal policies, procedures, guidance, and training as necessary to ensure these Privacy and Data Protection Principles are implemented.

1. *Fairness, Lawfulness, and Transparency:* BRG will consider the expectations of the Data Subject when processing Personal Data; will comply with Applicable Laws regarding Data Processing; and will provide transparent information to Data Subjects about how BRG Processes Personal Data.
2. *Purpose Limitation:* BRG will Process Personal Data only for specified and legitimate business purposes and will not Process Personal Data in a manner incompatible with those purposes.
3. *Data Minimization:* BRG will not collect or otherwise Process more Personal Data than necessary to accomplish the lawful purpose(s) for which the Personal Data was collected.
4. *Data Accuracy and Quality:* BRG will keep Personal Data accurate and, where necessary, up to date. BRG will take reasonable steps to rectify or erase inaccurate or incomplete Personal Data.
5. *Data Retention and Storage Limitation:* BRG will delete Personal Data when it is no longer needed for the purpose for which it was collected or required by law, regulation, court order, subpoena, or legal hold, consistent with BRG's Record Retention Policy.
6. *Data Security and Confidentiality:* BRG will implement reasonable and appropriate measures to secure the confidentiality, integrity, and availability of Personal Data.
7. *Data Subject Rights:* BRG will uphold Data Subjects' rights granted under Applicable Laws, including the rights to access, correct, or delete Personal Data.
8. *Accountability, Privacy by Design, and Privacy by Default:* BRG will incorporate these Privacy and Data Protection Principles into systems, products, and business processes by design and default. BRG will evaluate, implement, monitor, update, and document controls throughout the data lifecycle.

V. Governance

A. Privacy Team

The Privacy team is responsible for the implementation of this Policy and manages the operations of the Privacy Program. This includes:

- providing guidance on the application of this Policy to all BRG Personnel
- creating and implementing processes to continually improve and monitor compliance
- collecting data and metrics to measure the effectiveness of the Privacy Program

- providing employee training and education about Data Protection
- escalating known and potential risks to the appropriate level of management

B. Data Protection Officer

BRG has appointed a global Data Protection Officer (DPO). As needed or where required by Applicable Laws, BRG may appoint additional regional or subject-specific DPOs. The DPO(s) will advise on and monitor the Privacy Program for compliance with Applicable Laws and provide regular updates to BRG leadership. In consultation with BRG's Legal department, the DPO(s) may liaise with government agencies with jurisdiction over Data Protection issues.

C. Trust Office

Effective privacy and Data Protection require ongoing cross-functional collaboration to operationalize the principles described in this Policy. BRG has established a Trust Office that includes representatives of the Privacy team, the Legal department, the IT department, and Information Security team to ensure coordinated implementation of this Policy. The Trust Office, in its discretion, may engage additional BRG resources as necessary to accomplish privacy and Data Protection goals.

D. All BRG Personnel

All BRG Personnel will protect the privacy of Data Subjects whose Personal Data is collected or otherwise Processed by BRG in accordance with this Policy. Personnel will use Personal Data only for authorized purposes and as allowed under this Policy and Applicable Laws.

Personnel will complete periodic training on privacy and Data Protection as assigned.

VI. When to Contact the Privacy Team

In the following situations, Personnel should contact the Privacy team at privacy@thinkbrg.com or other channels that the Privacy team may designate.

A. When a Data Subject Request Is Received

BRG responds to DSRs as required by Applicable Laws. Depending upon Applicable Law, a Data Subject may request:

- access to or a copy of their Personal Data
- that BRG correct errors in their Personal Data
- that BRG limit how it uses their Personal Data
- that BRG delete their Personal Data

The above is a non-exhaustive list of DSR rights. Where Data Subjects are granted additional rights under Applicable Law, BRG will honor those requests.

While BRG asks that Data Subjects submit DSRs through specific channels, Personnel may receive DSRs submitted through any communication channel, particularly if you work in a function that

regularly engages in Processing of Personal Data for BRG, such as HR. If you receive a request from a Data Subject (or from a client on behalf of a Data Subject) asking to exercise any of the rights described above or asking BRG to do anything else with their Personal Data, contact the Privacy team immediately. The Privacy team will coordinate an appropriate and timely response.

B. When a Privacy Assessment Is Required

BRG proactively incorporates the Privacy and Data Protection Principles through privacy by design and privacy by default. Whenever Personnel are creating a new business process or onboarding a new system that involves Processing Personal Data, reach out to the Privacy team for a privacy assessment.

A privacy assessment reviews the proposed business process or system to identify, assess, and propose mitigations for potential privacy risks. In some circumstances, specific types of privacy assessments are required by law and must be completed prior to the start of Data Processing. Accordingly, Personnel are encouraged to contact the Privacy team early in the planning phase to avoid project delays.

C. General Advice and Support

BRG Personnel should contact the Privacy team with any questions or concerns about privacy at BRG.

VII. BRG as Controller and Processor

BRG, like other businesses, must Process Personal Data for its own purposes to operate its business. However, BRG is often entrusted with Personal Data belonging to our clients or other third parties. This creates important distinctions in how BRG goes about implementing this Policy.

A. Controller

When BRG has the authority and discretion to determine the means and purposes of Processing Personal Data, it is acting as a controller of that data. This includes things like Personal Data BRG collects and uses for recruiting, Personnel management, and marketing.

Where BRG acts as a controller of Personal Data, it has primary responsibility for many elements of Data Protection with respect to that data, including:

- providing proper notice of BRG's privacy practices
- collecting and maintaining records of consent, where required
- responding to DSRs
- conducting privacy assessments, where required
- notifying individuals and/or regulators or other government authorities in the event of a breach involving Personal Data

B. Processor

Given the nature of BRG's business, a large amount of the Personal Data we Process belongs to our clients, who entrust that data to us solely for BRG to conduct specific activities at each client's direction. In this situation, BRG's client is the controller of the Personal Data and has primary responsibility for the same elements of Data Protection as were described in the prior section. BRG's role as a processor of that data is to:

- Process the client's Personal Data only as directed by the client for the purposes they specify
- protect the client's data in compliance with Applicable Laws and BRG policies
- provide reasonable assistance to the client in meeting the client's obligations as a controller, where required

VIII. Compliance Documentation and Risk Management

The Privacy team will maintain an inventory of business activities that involve Personal Data. The Privacy team will update this inventory any time there are significant changes to business processes involving Personal Data or a new business process involving Personal Data is initiated.

Depending on jurisdiction, there also may be compliance documentation required for BRG's work as a processor of Personal Data for its clients. In those scenarios, the Privacy team will work with affected BRG functions to obtain the information necessary to maintain those records.

The Privacy team will conduct privacy assessments as may be necessary to identify and manage potential risks. The Privacy team will maintain a privacy risk register and will escalate risks to the appropriate level of management for review.

IX. Additional Policies, Procedures, and Guidelines

The Privacy team may create or approve additional policies and procedures in support of this Policy, as well as guidelines and training materials. These additional documents may, for example, provide more detailed compliance requirements related to certain laws, such as the US Health Insurance Portability and Accountability Act (HIPAA) or European Union General Data Protection Regulation (GDPR); provide specific guidance for business areas, such as HR or marketing; or address specific operational implementations, such as handling DSRs or conducting privacy assessments.

X. Compliance Monitoring

BRG's Privacy Program follows a cycle of risk assessment, risk mitigation, training, monitoring, and enforcement. The Privacy team will regularly monitor the Privacy Program, assess the Program's effectiveness, and identify areas for improvement.