GfK Privacy and Secruity Procedures

GfK Participant Privacy and Confidentiality

All survey responses will be maintained in a secure manner, with identifying information never revealed without respondent approval. All GfK panels who participate in the study will be given a copy of the Privacy and Term of Use Policy. In the privacy terms, there is a section entitled the "Panel Member Bill of Rights" which summarizes the confidentiality and privacy protections for panelists and explains that participants can decide whether to participate in the panel or to answer any survey questions. The Bill of Rights is also available electronically at all times to panelists via the panel member Web site. The "Bill of Rights" includes the following text:

- We are researchers, not telemarketers. Here's what we can promise you:

- We operate under the standards set by the Council of American Research Organizations (CASRO) [www.casro.org] and our Web site is approved by TRUSTe.

- Your survey responses and information are provided to our clients in an anonymous form, unless you have given your express permission.

- Occasionally, we may contact you to validate responses. We will never misrepresent ourselves, nor what we are doing.

- Your decision about participating in the GfK Panel or responding to specific questions will be respected without question.

The privacy terms also explain data security employed by GfK. GfK uses advanced security measures to protect against the loss, misuse, and alteration of information provided to GfK. To enhance data security, GfK Web server supports SSL (Secure Socket Layer) Encryption security technology and access to the GfK database is restricted to portals that only GfK controls. In addition, all panel members are required to use passwords and usernames.
GfK warrants that all employees are bound to protect the privacy and confidentiality of all personal information provided by respondents, and very few employees actually have access to any sensitive, personally identifiable data. The only staff members who have access to this information—personally identifying information about panel members—are those with a direct need to know. Therefore, the only persons with access are the following:

- Database and IT administrators with access to computer servers for the purpose of maintaining the computers systems at GfK;

- Staff members in the Panel Relations department that have direct contact with panel members as part of the inbound and outbound call center operations. These staff members are responsible for troubleshooting any problems panelists might be having with their equipment or software related to survey administration, incentive fulfillment, and panel management.

- Staff members of the Statistics department have access to personally identifying information in order to draw samples for the various surveys we conduct at GfK.

All personally identifiable records are kept secured in a separate office in the Informational Technology section of the main offices in Menlo Park, CA, and all data transfers from WebTV units and personal computers (both used for survey administration) to the main servers pass through a firewall. GfK never provides any respondent personal identifiers to any client or agency without the explicit and informed consent provided by the sampled Panel Members. Unless explicitly permitted as documented in a consent form, no personally identifying information will be provided to any parties outside GfK in combination with the survey response data.

All electronic survey data records are stored in a secured database that does not contain personally identifying information. The staff members in the Panel Relations and Statistics departments, who have access to the personally identifying information, do not have access to the survey response data. Meanwhile, the staff members with access to the survey response data, with the exception of the aforementioned database and IT administrators who must have access to maintain the computer systems, do not have access to the personally identifying information. The secured database contains field-specific permissions that restrict access to the data by type of user, as described above, preventing unauthorized access.

The survey response data are identified only by an incremented ID number. The personally identifying information is stored in a separate database that is accessible only to persons with a need to know, as described above. The survey data extraction system exports only anonymized survey data identified only by the Panel Member ID number. The data analysts with access to the survey data extraction system, as they do not have access to personally identifying information, cannot join survey data to personally identifying data. Panel Relations and Statistics staff do not have access to the survey data extraction system, and therefore cannot join survey data to personally identifying data.

As part of its prior work with RTI, GfK has implemented Good Clinical Practice guidelines to assure compliance with requirements for systems documentation and privacy of stored survey data. Consequently, a system of standard operating procedures have been put in place for documenting all processes relating to maintaining privacy of the identities of panel members. GfK retains the survey response data in its secure database after the completion of a project. These data are retained for purposes of operational research, such as studies of response rates and for the security of our customers who might request at a later time additional analyses, statistical adjustments, or statistical surveys that would require re-surveying research subjects as part of validation or longitudinal surveys.