GfK UK Ltd
Data Security Statement

GfK is awarded Certificate of Assurance and complies with the requirements of the Cyber Essentials Scheme. The accrediting body is the IASME Consortium.

GfK is awarded Certificate of Assurance and Complies with the IASME Information Security Standard. The accrediting body is the IASME Consortium.

The scope of the Cyber Essentials and IASME schemes applies to GfK UK and the GfK EMEA Data Centre in Nuremberg.

GfK wishes to reassure its clients that the security of the data it handles is of paramount importance. This statement has been written in addition to our existing policy statements on: Data Protection Act; Information Security; Freedom of Information; Business Continuity and Quality Management.

This statement should be read in conjunction with the GfK SE Data Security Statement.

- **Receiving, transmitting and storing personal data and sensitive personal data:**
  - GfK recommends that encryption is the benchmark for transmitting personal data and sensitive personal data. The method of encryption will reflect that required by our clients.
  - All inbound e-mail traffic for gfk.com is encrypted during the transmission (Transport Layer Security (TLS) protocol) - if the sender's mail system also offers this service. Outbound email traffic is protected by the corporate Exchange cluster and the smtp gateway mailout.gfk.com.
  - If a target system does not provide TLS, our servers automatically fall back to standard clear text transmission, but all attachments containing personal data and client confidential data will be encrypted.
  - GfK operates secure FTP sites for the transfer of data between ourselves and our clients.
  - Where data is to be transferred via a CD/DVD/hard drive, the data must be encrypted. If particularly sensitive we suggest serialising and sending a separate file with the serial number linked to name and address.
  - A Secure Courier Service only must be used and a named receiver given.
  - The sender must check the receipt of the data.
  - We would advise the client to only send information that is relevant to the task in hand. Any additional information that is not required for the research should be removed prior to the transfer.
  - Contracts / Instructions should be obtained from the client outlining deletion or retention criteria of the data.

- Contracts / Instructions must be provided to third parties outlining deletion, retention, transfer and security requirements of the data.

- **Recommended Project Record Retention**
  - The following retention periods apply to survey data unless the client requires otherwise and clearly documents that to us.
    - 1 year (or less) - Primary records (sample, completed questionnaires, etc)
    - 2 years - Secondary records (reports, presentations, output to client, etc)
  - These are based upon the requirements of ISO 20252, the international standard for market, opinion and social.

- **All staff must comply with:**
  - GfK Global Information Security and Privacy Guidelines
  - GfK Global Technology Use Guidelines
  - GfK Global Social Media Policy
  - All staff undergo initial inductions on information security and data protection, and on-going awareness and update training, as appropriate.

- **Data held within GfK**
  - GfK operates a highly secure network environment with firewalls and IPS systems to ensure no unauthorised access to the network is gained.
  - Only GfK owned or managed devices are permitted access to the GfK Internal network from the WAP.
  - Secure access protocol such as https, sftp or ssl is used on all WiFi
  - GfK operates tiered storage architecture and data is stored on the appropriate device according to the criticality of the information. A data management policy defines the types of data and where it should be stored and protected depending on the criticality of the data to the business.
  - Access to data is limited to only those individuals who require it in order to carry out our services for you.
  - Directories are established to ensure different client data / team directories are logically segregated and all access to files is controlled
  - Access to information is granted on an ‘as needs’ basis which has to be authorised by the data owner.
  - All Users have a unique User ID and password.
  - We use ComVault for virtual back-ups which means the data remains within the GfK IT Infrastructure, UK data is backed-up to the GfK Data Centre in Nuremberg over a private link, and access to it controlled using Active Directory.
  - All GfK UK Laptops have hard drive 256 bit encryption. All Computer Assisted Interviewing Devices used by our Field Interviewing Force have hard drive encryption.
  - All web sticks and other mobile devices also have encryption employed.

- **Physical security**

- Visitors are supervised at all times; 24 hour minimum notice of visitors is a requirement at the Head Office
- We have a Proximity Card System for access to the building, which also limits access to specific floors and areas within the building. Passport style photographs are required for the proxity cards and the photos are checked by the building security.
- 24x7 on-site security guards.
- CCTV monitoring of external perimeter and external access points.
- No externally facing windows for computer facility or sensitive processing areas.
- Agile working ensures a complete clear desk policy with each individual assigned a locked cabinet.
- Adequate fire protection is in place.
- Physically segregated access zones, such are the computer room, exist within the building and have CCTV coverage on entries
- Access to the computer room(s) restricted to authorised persons.
- Access by external personnel (service and telecom engineers, cleaners etc) restricted and supervised.
- All servers and network components are racked appropriately unless self-standing.
- The environmental services within the Canada Square server room(s) are monitored 24/7 *365.
    - This is performed by the Canada Square building services team.
- Locked confidential waste bins across all floors, data is shredded weekly.

Definitions

Personal data: any information that relates to and identifies a living individual – this can be name, address, post code, job title, email address, recorded image, etc.

Sensitive personal data: race or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life, the commission or alleged commission of an offence or any proceedings for an offence committed and the outcome.

Confidential data: any other business critical information.