GfK SE
EMEA IT Shared Service Centre

Data Security Statement

The IT Shared Service Centre EMEA (Europe, Middle East, Africa) is a Division of GfK SE Data Services in Nuremberg. The IT Service Centre EMEA provides the hosting and support of the following services across GfK Group European Companies:

- Corporate Web Site
- Client Portals
- Application Hosting
- Corporate E-mail (mail boxes, mail scanning, Blackberries, Outlook Web Access)
- FTP (File Transfer Protocol) and secure FTP
- Remote Access (SSL VPN)

The IT Shared Service Centre EMEA follows the security practices defined in the GfK Global Information Security Policy. The GfK Global Policy for Information Security is based upon the control objectives and best practice security framework as documented in ISO/IEC 27001:2005, Information technology -- Security techniques -- Code of practice for information security management. Its objective is to provide management direction and support for information security within GfK, to facilitate protection to the business and confidence when dealing with outside companies.

The policy covers the following areas:

- Information Security Organisation
- Compliance with Legal and Contractual Requirements
- Personnel Security
- Desktop Security
- Incident Reporting
- Secure Areas
- Asset Classification and Control
- Equipment Security
- Security of Third Party Access
- System Planning and Acceptance
- Computer Operational Procedures and Responsibilities
- Protection from Malicious Software
- Data Backup
- Media Handling and Security
- Network Management
- Information Exchanges
- User Access Management
- Application Access Control
- External Connections
- System Development and Maintenance

This statement should be read in conjunction with the GfK EMEA Data Centre security statement that outlines the Physical and Environmental security of the facility.

- **Security of Data held in the EMEA Shared Service Centre**

- GfK operates a highly secure network environment with firewalls and IDS systems to ensure no unauthorised access to the network is gained.
- GfK companies are connected to the Data Centre over a secure private MPLS network, provided by Level 3 or via VPN connections managed by GfK
- Only GfK managed equipment is permitted access to the network
- The EMEA Data Centre operates tiered storage architecture and data is stored on the appropriate device according to the criticality of the information.
- 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 credentials.

- Passwords are changed every 90 days and must be complex.
- Back-up tapes containing client data are encrypted using industry standard AES-256 encryption algorithm.
- Data is backed up on a daily basis. There are daily incremental backups and weekly full backups.
- All backup media is kept off site at another GfK facility
- Backups are retained for 30 calendar days and then overwritten. It is possible to recover any data over the last 30 days.
- Longer retention times are called archives and can be designed to meet clients' specific requirements.
- All Servers, desktop and laptops have anti-Malware controls in place
- The Anti-Virus scanners are centrally managed and updated daily
- Laptops have a local firewall installed and hard disk encryption to protect the information store on the machine

- **Receiving, transmitting and storing personal data and sensitive personal data:**

- GfK recommends that encryption should be used when transmitting personal data and sensitive personal data. The method of encryption will reflect that required by our clients.
- All inbound/outbound e-mail traffic for gfk.com is encrypted during the transmission (Transport Layer Security (TLS) protocol), if the sender's mail system also supports this service.
- If a target system does not support TLS, our servers automatically fall back to standard clear text transmission. Staff are instructed to encrypt any attachments containing personal data or client confidential data unless they know the recipient mail system support TLS.
- All external e-mail is scanned in two stages by different malware protection vendors
- In addition the mail client are protect with a local Anti-Virus scanner
- GfK operates secure FTP sites for the transfer of data between us and our clients.
- Where data is to be transferred via a CD/DVD, the data must be encrypted. If particularly sensitive, the data should be serialised and sent in a separate file with the serial number linked to name and address.
- A Secure Courier Service must only 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 before 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.