

As the UK Information Commissioner calls for companies to conduct "privacy impact assessments" here at GfK NOP we want to reassure our clients that the security of the data we handle is of paramount importance to us. This statement has been written in addition to our existing internal policy statements on: Data Protection Act 1998; Information Security; Freedom of Information Act 2000; Business Continuity and Quality Management

Receiving, transmitting and storing personal data and sensitive data:

This includes receipt of data from the client and transfer of data to a third party processor, where applicable

- We recommend to our clients that encryption is the benchmark for transmitting personal data and sensitive data.
- Where possible we can operate a secure FTP site for the transfer of data between ourselves and our clients.
- Where encryption is not compatible a minimum requirement is to password protect the files to be transferred and to separate the data within a database / sample file. That means, sending the identifiable data coded in a separate, password protected file that contains a serial number and not name and address details.
- Where data is to be transferred via a CD/DVD, the data should 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 and that no additional information that is not required for the research.
- Contracts / Instructions should be obtained from the client outlining deletion or retention criteria.
- Contracts / Instructions must be provided to third parties outlining deletion, retention, transfer and security requirements.

Data held within GfK NOP

- GfK NOP operates a highly secure network environment with firewalls and IDS systems to ensure no unauthorised access to the network is gained.
- GfK NOP 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.
- All data is backed up daily and stored in a secure off-site vault.
- All GfK NOP 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.

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.

1. Clients must be registered under the Data Protection Act to be able supply customer data (name / address / telephone number and any other customer details) for “research” purposes. You can check the client’s registration at <http://www.esd.informationcommissioner.gov.uk/esd/search.asp>
2. All respondents must have given their permission for their details to be passed on for research purposes – either as an opt-out or opt-in, depending on what method the client has chosen to record this.

An example question to ask is “From time to time we might pass on your details to a third-party for market research purposes, please tick the box if you do not want this to happen. ” – the opt-out.

3. Clients must record the answers to the above question in such a way that data supplied (whether sample or a data set for data matching purposes) omits the respondents who opt out / have not opted in.
4. Clients need to consider how to respond if any customers query the right to transfer their details to an agency to use for market research purposes.

Full guidelines are available from the MRS (www.mrs.org.uk) entitled **Market Research Processes (Client) and the Data Protection Act 1998**.

<http://www.mrs.org.uk/standards/downloads/revised/legal/mrprocesses.doc>



