



& AURA

Market research processes (client) & the
Data Protection Act 1998
January 2004

CONTENTS

	Page
Introduction	3
Section A: Principles of the Data Protection Act 1998	4
Section B: Research Project Processes	5 – 14
1. Commissioning	
2. Project Design & Execution	
3. Processing, Analysis, Reporting & Storage of Data	
4. Use of Data	
Appendix 1: Data Protection Act 1998 – Principles and Definitions	15 – 17
Appendix 2: Notification Procedures	18 – 20
Appendix 3: Categorisation of Data Collection Projects	21 – 23
Appendix 4: Client Action Plan (including contract checklist)	24 – 25
Appendix 5: Data Protection Scenarios	26 – 28

INTRODUCTION

During the whole of 2002 the MRS Codeline service received 90 queries on data protection, in the first two months of 2003 the service received 30 queries on the same subject. This illustrates just how important data protection has become in the everyday activities of researchers.

The Data Protection Act 1998 is good for the market research industry for four important reasons:

- Legal commentators see the UK version of the Directive as providing a very good balance between preventing the exploitation of personal data whilst respecting the value of such data within the modern world. We also have a regulatory framework that welcomes discussion first rather than seeking confrontation when issues emerge;
- Market research, as defined within the Code of Conduct, continues to enjoy exemptions from certain aspects of the legislation, and the industry has been able to successfully (twice) stop challenges to re-define part, or all of the industry, as direct marketing;
- It gives more weight to the Code, in particular those key clauses that are designed to protect the rights of respondents - first established by the industry world-wide over fifty years ago;
- Because of the legal implications, it focuses the industry on improving the overall standards of the research process thereby maintaining the trust of all those who come into contact with the industry, whether as respondents, clients, readers of research findings, legislators and regulators.

It is therefore vitally important that all those within the market research industry, and those that use its services, meet the requirements of this legislation.

The purpose of the following guideline is to provide advice and guidance on the Data Protection Act 1998 for those working in market research departments or others who commission market research projects. (Note: Any client organisation that also undertakes its own research, for example, has its own field or telephone interviewer force, or undertakes on-line research, should also ensure that they are familiar with the MRS/BMRA process guidelines referred to in the final paragraph of this Introduction).

It is likely that client organisations have an individual, or department, responsible for ensuring that the organisation meets the requirements of data protection legislation. This should be the first source of help. However, in most client organisations, market research will not be a core activity and therefore those responsible for data protection may not be fully aware of how the legislation impacts on this activity, or the important distinctions between confidential survey research and other uses of personal data to support marketing activities that are more closely regulated by the 1998 Act (direct and database marketing). This guideline will therefore be helpful in ensuring that organisations make the right decisions when commissioning market research projects.

The guideline is based on the detailed advice for Market Research Society (MRS) members contained within ***'Market Research & the Data Protection Act 1998: Advice for Members'*** (this contains an important new categorisation of data collection to meet the requirements of the 1998 Act) and, ***'Draft Guidelines for collecting data for mixed or non market research purposes ('Category 6')***. These guidelines also complement the guidelines on how the 1998 Act impacts upon market research agency processes ***'Market Research Processes and the Data Protection Act (DPA) 1998'*** produced by the MRS and the BMRA. For full details of all these guidelines see www.mrs.org.uk. **Also, specific industries may have guidelines and interpretations of the Data Protection Act 1998 that may apply to market research (e.g. the banking and pharmaceuticals industries – see the Code/Guideline section of the MRS website for more details).**

SECTION A: PRINCIPLES OF THE DATA PROTECTION ACT 1998

All processing of personal data must conform to the requirements of the 1998 UK Data Protection Act (for more information see www.dataprotection.gov.uk).

Appendix 1 summarises some of the key points within the 1998 Act:

- The eight data protection Principles within the Act that form the fundamental basis of the legislation;
- Key definitions contained within the legislation plus how these definitions apply to market research;
- Notification procedures for market research purposes.

The key rules underlying the Act are:

- **Transparency** – ensuring individuals have a very clear and unambiguous understanding of the purpose(s) for collecting the data and how it will be used;
- **Consent** – at the time that the data is collected, individuals must give their consent to their data being collected, and also at this time, have the opportunity to opt out of any subsequent uses of the data¹.

When collecting research data the purpose of the data collection must be transparent. Data collected only for **confidential (market) research** purposes must only be used for that purpose. If data is to be collected for other, or mixed, purposes (e.g. database enhancement, staff training etc) this must be explained to respondents when the initial contact is made (see the section on Category 6 projects).

If a respondent's details are to be *kept* on a client or agency held database for a further interview, the respondent must be made aware of this at the initial interview and given the option not to be re-contacted.

To help market researchers and their clients understand how the 1998 Act and the MRS Code of Conduct affects the permissible flow of personal level data from market research projects, the industry has developed a new categorisation of feedback. These new categories are summarised within Appendix 3.

Essentially, keeping within the 1998 Act when undertaking market research needs a common sense approach. Place yourself in the respondent's shoes when designing or conducting a market research project. If as a result of participating in a survey, a respondent's personal data is used for any purpose that, from the respondent's perception, would be unexpected then it is possible that the law may have been broken. Three examples:

- re-contacting a respondent for a further interview without having raised the possibility and asking for their consent to do so during the initial contact;
- transferring a respondent's personal data to an agency other than the one(s) in whose name it was collected in the first place without have gained their consent in the initial interview;
- Using a favourable opinion given by a respondent during a confidential market research interview as an identifiable testimonial on marketing materials without the permission of the respondent.

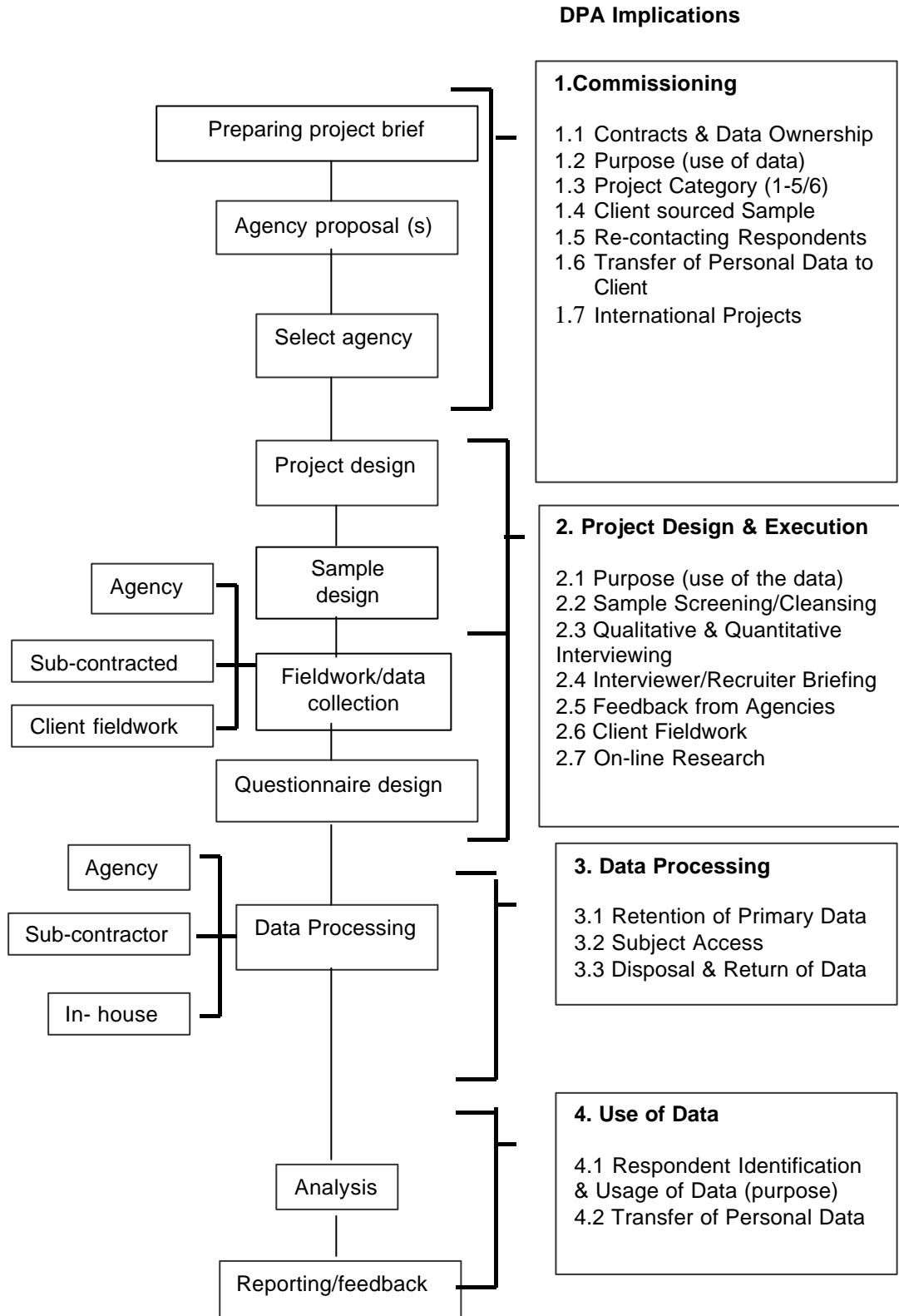
The MRS guidelines, 'Market Research and the Data Protection Act 1998: Advice for Members' includes a list of frequently asked questions and answers relating to the legislation, including the Notification procedures.

¹ This does not apply to any re-analysis of the anonymous data as long as individuals cannot be recognised.

SECTION B: RESEARCH PROJECT PROCESSES

The following chart covers the research project process from a client perspective. Each of the key data protection implications is then described within the numbered sub-sections.

Data Protection Act 1998 and The (Client) Research Process



1. COMMISSIONING

At the time of preparing a project brief and reviewing agency proposals, several factors must be considered to ensure that the data protection requirements have been met. Depending on whether the client is supplying the data for sampling or it is supplied from another source will dictate how the following will be applicable for any project.

1.1 Contracts & Data Ownership

- Data controllers should always draw up legally enforceable contracts before releasing data to agencies (or data processors). Client organisations should have standard clauses covering the appropriate issues (see Appendix 4 for guidance on contracts).

The Act requires that agreements, preferably a legal contract, with data processors be evidenced in writing. The following are some action points to consider if you, or an agency acting on your behalf, are commissioning a data processor:

- Prepare clear and concise standard data protection clauses.
- Review existing contracts with subcontractors to ensure that any liabilities caused by their activities are passed on.
- Select subcontractors who can meet your standards.

Clients have data protection obligations when conducting market research. When the client supplies data for a sample frame the following conditions apply:

- The client must have completed their annual notification with the Office of the Information Commissioner (OIC).
- The notification must ensure that data is used for “research” purposes. The notification details can be checked via the Notification Register on the OIC website (www.dpr.gov.uk).
- If the project includes data collection for purposes other than purely for confidential survey research (such as direct marketing) the client must include this additional purpose(s) in the Notification.
- Clients should check that the agency is aware of their responsibilities (and those of any sub-contractors) under the UK Data Protection Act 1998.
- Clients should ensure that contract/terms and conditions contain clauses that adequately cover the data protection responsibilities of agencies and any subcontractors. Such as the need to ensure that any personal data provided by clients (e.g. customer records used for sampling) will be securely held; not used for any purpose other than as specified by the client in undertaking the specific project; destroyed or returned to the client once the project has been completed.
- Clients need to consider whether or not agencies/sub-contractors are likely to become joint (with the client) data controllers of any client supplied data, for example, a personalised database containing customer details plus survey findings and ensure that this is clearly defined and reflected within the contract.

(See the BSI Guide to Data Controller and Data Processor Contracts (2001) for more details).

1.2 Purpose (use of data)

Clients should clearly state within the brief if the personal data collected within the project is to be used for purposes other than confidential survey research (see guidelines for Category 6 projects).

1.3 Project Category

The brief should refer to the appropriate categories of data collection contained within the MRS data protection guidelines in order to define the type of project and the feedback required from the agency.

1.4 Client Sourced Sample

It should be noted that any breach of the Act that occurs while personal data is held by a market research organisation, on the client's behalf, e.g. a list supplied by a client for sampling purposes, would result in the **client** being liable for the breach – unless a contract has been agreed where the agency accepts responsibility. In serious cases clients would have to answer to the Information Commissioner or the courts. In addition any compensation that might have to be paid to a data subject/respondent as a result of a breach of the Act by a research organisation would result in the owner of the data (the client) paying the compensation. Therefore it is essential that clients check that market research organisations have adequate security processes to meet clients' and the Acts needs.

If a client owned file or database of customers is to be used for sampling purposes, then clients need to consider the following:

- The Notification covers market research and that appropriate safeguards are in place within the contract to cover security and prevent misuse by third parties (*see Appendix 2 for Notification procedures*).
- If feedback is required (Categories 2/3/4), then this should be specified.
- If it is a Category 6 project then the file will need to be screened as described in the guidelines.
- In instances where a client has supplied their own database for sampling the respondent has the legal right to know the source of the data if it is requested.

If sub-contractors (e.g. fieldwork agencies, freelance recruiters, data processors etc) are to be used then only those contractors who can offer appropriate safeguards (for security etc) must be retained. This condition applies to all stages of the market research process including interviewing.

- Market research organisations must offer sufficient assurances that they have appropriate technical and organisational measures in place to safeguard the personal data passed to them for processing.
- Any agreement to send data from a client to a market research organisation must be evidenced in writing.
- Clients need to consider how to respond if any respondents drawn from a client supplied list query the right to transfer their details to an agency to use for market research purposes. The client Notification covering the source must include market research.
- Care should be taken if known ex-directory numbers are to be included in a telephone survey; any relevant opt-outs should be respected. Best practice would be to screen them out

when selecting the sample, but otherwise interviewers should be briefed on how to respond to any queries/complaints from contacts.

- Samples for Category 6 projects must be fully screened.
- If one or more separate client organisations or legal entities (for example, separate companies within a group) are planning a joint survey using samples drawn from their respective databases, then personal data about respondents cannot be shared across these entities without the consent of respondents. This only applies to attributable data. It is therefore preferable if the merging is undertaken by the market research agency.

1.5 Re-contacting Respondents

The Data Protection Act 1998 specifies a number of conditions that must be met before processing is considered “fair” (the first data protection principle). One of the requirements is that respondents are aware of the likely consequences of participating in a data collection exercise. If a respondent’s details are, or likely, to be used for a further interview (apart from quality control checks), the respondent must be made aware of this at the initial interview and given the option not to be re-contacted.

1.6 Transfer of Personal Data to Client

Data Protection legislation is only applicable to data that identifies an individual. Aside from information such as name, address, national insurance number, email address or telephone number, this also relates to other information which reviewed together could identify an individual e.g. job title and employer.

At the planning stage:

- The client must discuss with the agency whether identifiable data is to be passed to the client. Identifiable data can be collected and passed to a client during a market research exercise on the condition that it is used only for the purpose for which it was collected (e.g. market research purposes), and, if the data is collected under the name of the agency the respondent must have given their consent to this transfer.
- The client needs to decide whether the project will be conducted in the name of a third party rather than the name of the client (i.e. a research agency), or that of the client as personal data cannot be passed from the agency to the client without the permission of the respondent if the survey is conducted purely in the name of the agency (see Category 5).

1.7 International Projects

Any identifiable data sent outside of the EEA, other than for processing purposes, requires one of the following conditions:

- the country has been approved by the European Commission as having adequate levels of data privacy legislation
- contract with the receiver that they have adequate data security to meet the requirements of the Data Protection Act 1998;
- consent of the data subject;
- the receiver signing up to the US “Safe Harbor” agreement (this applies to US companies only – see www.export.gov/safeharbor/ for more details).
- The organisation must always ensure adequate security of personal data during storage and transfer. Particular care is required when personal data is stored or transferred via the Internet.

- Clients should:
 - agree with the agency if the data is to be transferred;
 - define where the data is to be transferred;
 - agree appropriate permissions, if necessary, in the questionnaire to allow the data transfer to take place and/or include in the contract with the data recipient standard data transfer clauses (see www.europa.eu.int/comm/internal_market/en/dataprot/news/index.htm for standard data protection clauses).

Clients based in the EEA should note that if they are registered as data controllers for personal data concerning non-EEA citizens (e.g. residents in non-EEA countries), then the EU Directive legislation applies to any research surveys conducted amongst them. Similarly, if a company has its registered offices outside the EEA, but has a formal presence in the EEA (e.g. regional office), then the Directive covers the collection of any personal data within the EEA.

2. PROJECT DESIGN & EXECUTION

2.1 Purpose

All market research projects need to include a clear statement of the purpose (i.e. 'confidential survey research', and what this means in terms of protecting the identity of the respondent).

For Category 6 type projects, the questionnaire must include a statement that details any additional purposes that the data will be used for. If direct marketing is one such purpose then a question offering the respondent to 'opt out' of this purpose must be included.

2.2 Sample Screening/Cleansing

In instances where a client supplies a market research organisation with data for sampling, the following must be considered:

- The types of data subjects (e.g. business or private customers; adults or children etc) included on lists supplied by the client
- Use of personal data held by other divisions within a company, or subsidiaries, (e.g. a customer sample drawn from multi-sources) may require the prior permission of the data subjects concerned if any of the sample sources used are not Notified for market research purposes.
- Whether the list includes ex-directory numbers for a telephone survey (see 1.4 for further guidance).
- Ascertain when the list was last cleaned.
- Any known problems with the list.
- Any pre-existing "opt outs" permissions that are present in the file must be reviewed. There is no legal requirement for market research to be included in the opt out permissions. However if a client decides to include market research as an opt out, the rights of the data subjects must be respected and all those who have indicated they do not wish to be contacted for market research must be screened out of the sample provided to the market research organisation.
- There is no legal requirement to screen market research samples against the preferences services (such as the Telephone Preference Service) when conducting market research. However clients may have a policy regarding whether they wish to contact such individuals and this should be investigated at the proposal planning stage.

- Where the project is Category 6, then the sample must be fully screened firstly for opt-outs for direct marketing held on the database and secondly against the Direct Marketing Association's preference service databases.

2.3 Qualitative & Quantitative Interviewing

A key requirement of the Data Protection Act 1998 is that respondents are informed about the research study to which they are invited in a clear and unambiguous way. They must not be misled into agreeing to participate in the research. Points to remember:

- It must be made clear who the data collector is and for whom the data is being collected e.g. by a recruiter or an interviewer on behalf of a research agency or a client. All recruiters or interviewers, whether working on the telephone, via email or face-to-face, must make it clear who will be conducting the group, depth or interview and who will "own" the personal data - this could be either the agency or the client. (For example one approach could be providing the information in the preamble to a survey: 'Good morning, I am working for XYZ research company on behalf of ABC Ltd. We are conducting a market research survey about your attitudes as a customer of ABC Ltd.....').
- During the qualitative recruitment process:
 - Respondents must be informed of the subject(s) of the discussion or interview as precisely as possible compatible with the objectives of the study
 - Respondents must be notified beforehand if a qualitative discussion is to take place in viewing facilities and when it is to be recorded. All documentation given to the respondents (invitations etc) must always make reference to audio and visual recording.
- When sensitive data (as defined in the Act – see Section B clause VII) has been collected extra care should be taken to ensure that unauthorised individuals do not access the data. Agencies should consider adopting encryption measures on CAPI machines.
- When obtaining the respondent's consent for recording (e.g. tape and video data collection) the purpose of making the recording (e.g. for research purposes) must be stated.
- When recruitment or interviewing is conducted from lists, it is incumbent on the interviewer/recruiter to inform any respondent who requests the information, the primary source of a list. Where a client supplies a data list and the client does not wish their identity to be revealed, because it would adversely affect the research for respondents to have such prior knowledge, the researcher can agree to reveal the identity at the end.
- If a respondent at any stage withdraws their consent e.g. at the end of a group discussion, the respondent's contribution to the research must be suppressed from the final analysis and reporting.
- Any people observing a group must be made aware that the content of the discussion contains personal data and should not be disclosed in any way that could identify a particular individual participant.
- Any transcripts or tapes must be used for confidential market research purposes only, unless prior permission is gained from respondents. If the data is required for any other purpose then the project must adhere to the conditions described within the Category 6 guidelines.
- If a subject access request is received for recorded data the information can be supplied in alternative formats (such as a transcript) unless all those included in the recording have given their consent for the recorded information to be released.

2.4 Interviewer/Recruiter Briefing

The DPA98 requires researchers and their sub-contractors to take responsibility for the security of personal data provided to them. This has implications for all material where personal information has been supplied and where this is tied to a specific individual such as on a recruitment questionnaire, self-completion questionnaire, pre-placed materials or any other documentation that has been completed by an interviewer, recruiter or respondent. Clients should therefore check that interviewers working on the project are adequately briefed about their data protection responsibilities. Therefore, clients need to ensure that the contract with any agencies or other data processors covers this issue, including the following points:

- Once data has been collected and received the following points should be considered:
- Client customer lists:
 - These must be stored securely during use.
 - All hard copy and electronic address lists must be: stored securely; destroyed; shredded; or returned to the client. The information contained within them must not be used by interviewers to help recruitment of respondents for future projects for other clients (i.e. to build respondent recruitment lists/databases).
- If recruiters are used to recruit respondents:
- The personal data they collect can only be used for the contracted research project and for no other future projects.
- Questionnaires/documentation with identifiable respondent data:
- Questionnaires must **never** be handed to the client, either during or after an interview without the express permission of the respondent.

2.5 Feedback from Agencies (inc Sample Cleansing)

If a supplied list contains incorrect information relating to a respondent for example an incorrect address or telephone number, or if they have died, then this information can be fed back to the client. It is incumbent on the interviewer/recruitment agency, and in turn the research agency, to inform the client that the data is incorrect but in the case of incorrect addresses the corrected data cannot be supplied without the express permission of the respondent – that is, the agency can tell the client that an address etc appears to be incorrect, but the client is responsible for finding out the correct information and amending their database. This is because under the 1998 Act it is the responsibility of the data controller to ensure that the information held in their databases is accurate and up-to-date. The Act does not cover those who have died and therefore this information can be fed back.

- Details of incorrect data must be fed back to the client as soon as possible.
- The client has a responsibility under the fourth data protection principle to ensure that data is accurate and up-to-date. If a sample frame owned by a client contains a high number of incorrect records then the client should conduct a data cleansing exercise.
- 'Gone away' information collected during a survey should not be used for other purposes (e.g. a utility cannot use this information to build a database for marketing purposes).
- Clients can also request a list of those who have been contacted, solely to place markers on their database to prevent over researching individuals – but these markers must be used for research purposes only.

- Details of specific dissatisfactions/complaints can be fed back to clients, with the consent of the respondent, for resolution. These will be fed back by the agency separately from the research findings. The information must not be used for any other purpose.

2.6 Client Fieldwork

Clients undertaking their own field work should also be familiar with the MRS/BMRA guideline, 'Market Research Processes and the Data Protection Act (DPA) 1998'.

2.7 On-line Research

If a client undertakes its own on-line surveys, then the web sites must contain sufficient information regarding the market research policy. The Information Commissioner has produced a set of general guidelines for company web sites and the MRS and ESOMAR have developed guidelines covering market research (see respective websites for details).

3. PROCESSING, ANALYSIS, REPORTING AND STORAGE OF DATA

3.1 Retention of Primary Data

Once data collection has taken place the security of the data should be maintained:

- All identifiable data must be held securely without any unauthorised access. If a respondent suffers either distress or damage as a result of data being used in an inappropriate manner the respondent can claim for compensation.
- If data is held off-site at an archive storage facility the security measures must be appropriate and adequate to meet the security needs of the client data stored.

Clients should ensure that agencies do not retain primary data (e.g. questionnaires) longer than is absolutely necessary:

- The client and the agency should agree a data security, retention and destruction policy within the original contract and these conditions must be met.
- An example of a retention period: for an ad hoc project it may be possible to destroy the personal data after three months; for a respondent who is no longer on a continuous panel, then the period may need to be longer

3.2 Subject Access

When clients or their market research organisations hold respondent information in an identifiable format, the respondents have the right to see the personal data held about them. This includes any data held on computer files, manual data (such as questionnaires) and any audio/video images. The process of respondents requesting data held about them is known as a "subject access request". When data is held in an unidentifiable format the data falls outside the definition of personal data and thus subject access rights do not apply.

- If a subject access request is received a client or their market research organisation may have to comply and provide copies of all identifiable data held about a respondent. If the task would be of a disproportionate effort and costly to fulfil for either the market research organisation or the client they may not have to satisfy the request.
- For a subject access request personal data does not have to be supplied in the same form as it was collected e.g. a transcript of a recorded group may be supplied rather than the recorded data.

- When providing information about subject access requests it should state that it is only necessary to meet the requirements of the request if it is received in writing. There is a timescale in which the request must be responded to (40 days from the written request) and the data controller can request more information from the data subject in order to clarify their subject access request before the 40 day time period legally begins.
- The 1998 Act permits a small fee of no more than £10 can be charged by the data controller for the subject access request. It is at the discretion of the Data controller if a fee is to be charged and this should form part of a client's and/or agency policy on data protection.
- Clearly label and store project data (includes manual and tape data held) to ensure that information can be retrieved on receipt of a subject access request.

3.3 Disposal & Return of Data

The contract with the agency should clearly specify whether any personal data supplied by the client should be destroyed or returned to the client.

For quality standard purposes it is only necessary for agencies to keep primary data which is required for the analysis of the data and report preparation. Points to note are:

- All hard copy and electronic address lists must be held securely by the agency until either these are returned to the client or destroyed by the agency.
- Clients should check that the research organisation ensures that similar procedures are in place for any data held by sub-contractors involved in a project (e.g. interviewers and recruiters).
- Clients should ensure that the destruction of the data is adequate for the confidentiality of the data being destroyed. For example any data that contains personal data should be confidentially shredded.
- Where a permission to re-interview question has been included, the personal data collected in the original interview may need to be retained until after any subsequent contact has been made.

4. USE OF DATA

4.1 Respondent Identification & Data Usage (Purpose)

Questionnaire text must have been sufficiently clear to ensure there was no ambiguity when gaining permission from the respondents.

- The identity of respondents and/or the use of attributable comments can only be used with the express permission of the respondent.
- Clients must not use the data for purposes other than those stated to respondents at the time of data collection, and any opt-outs must be respected (Category 6 projects). In particular, data collected for confidential market research purposes only, cannot be used for any other purpose (e.g. staff training, database enhancement, list building etc).
- Respondents must not be harmed as a result of using data in this way (e.g. during a banking customer satisfaction interview a respondent criticises the performance of a particular member of staff. These comments are fed back to the individual who then confronts the customer when they next visit the branch).
- Care must be taken if data from a survey is used to develop models for use in an anonymised market research database to ensure that individual respondents cannot be identified. For example, it could be possible to identify an individual customer at full post-code level:

- if they were the only customer within that postcode;
 - if the unique characteristics of customers within a postcode, such as purchasing behaviour enabled individuals to be identified.
- Particular care is needed when using samples drawn from small universes.

4.2 Transfer of Personal Data

Data can be transferred to third parties only with the consent of the respondents at the time of the initial data collection.

- If the data is to be transferred outside of the European Economic Area the respondents must have consented to this or data transfer clauses must be incorporated into any written contract (*see section A clause 1.9 for details*).
- Transfers of personal data (e.g. customer data) from one legal entity to another within the same overall company, or group of companies, may require prior permission from the individuals concerned.
- For audio, video recordings or transcripts to the client:
 - All individuals recorded must have consented to the recording or the transcribing, and the subsequent release of the data to the third party and the purpose to which the recording will be put by the third party.
 - If an individual withdraws consent after the group or interview takes place, the researcher must not pass the data to the client.
 - When primary data is released it must be labelled with the details on the purposes for which it can be used.
 - The recipient of personal data must not use it for any purpose other than that for which it was collected
 - Such conditions should be stated in some form of contract between the client and the researcher.

Appendix 1

DATA PROTECTION ACT 1998: PRINCIPLES, DEFINITIONS AND NOTIFICATION PROCEDURES

PRINCIPLES

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
 - at least one of the conditions in Schedule 2² of the Act is met, and
 - in the case of sensitive personal data, at least one of the conditions in Schedule 3³ is also met
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or other purposes
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
4. Personal data shall be accurate and, where necessary kept up to date (with every reasonable step being taken to ensure that data that are inaccurate or incomplete, having regard to the purpose(s) for which they were collected or for which they are being further processed, are erased or rectified)
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
6. Personal data shall be processed in accordance with the rights of data subjects under this Act
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

DEFINITIONS

I. Personal Data

This legislation only covers data that identifies a living individual. Data that is covered by the Act includes electronic, manual and recorded data - anything that can identify an individual. Once any identifiers linking data to an individual have been destroyed and it is impossible to identify that individual then it no longer constitutes "personal data" and is therefore not covered by the provisions of the 1998 Act.

² Additional conditions known as schedule 2 and schedule 3 have been added to the first principle. Schedule 2 sets out the basis on which the collection and use of data is permitted. They are,

- the individual agrees to the processing
- the processing is necessary
 - for the performance of a contract
 - for compliance with a legal obligation
 - to protect the vital interests of the individual
 - for the exercise of a public function in the public interest
 - for the data controller's or a third party's legitimate interest unless prejudicial to the interests of the individual.

³ Schedule 3 of the first principle adds further conditions on processing if the data is "sensitive". See *Section B for full details*.

II. Data Subject

The data subject is the individual who can be identified directly or indirectly by the data collected. In particular by reference to an identification number or the person's physical, physiological, mental, economic, cultural or social characteristics.

III. Notification

This is the process of informing the Office of the Information Commissioner (responsible for the Data Protection Act 1998) about personal data held and processed by the data controller. The Information Commissioner maintains a public register of data controllers. Each register entry includes the name and address of the data controller and a general description of the processing of personal data by a data controller.

Any client owned databases containing details of customers would need to be notified, and, if they are to be used for deriving survey samples, then the entry on the register needs to include confidential market research as a purpose for which the data will be used.

See Appendix 2 for further details on notification procedures.

IV. Data Controllers

Data controllers are those who control and determine the use of personal data they hold and the manner in which any personal data are, or are to be, processed. All data controllers must 'Notify' their activities with the Office of the Information Commissioner (OIC).

V. Data Processors

A data processor is any person (other than an employee of a data controller) who processes data on behalf of a data controller, but has no right to use the data for any purpose (e.g. in the context of market research this may cover organisations that undertake fieldwork only or data processing).

It is unlikely that a market research agency will act solely as a processor when undertaking client projects as they will be creating files or databases containing personal data which will remain within their control – this will also apply where a client has provided a customer file for sampling purposes if the agency uses this as a master file for the projects. Clients and agencies may therefore both become separate data controllers for databases containing some of the same data. Similarly clients and agencies may be joint data controllers for data sets that are shared between two parties (e.g. with some panel data).

For example:

- Sample file provided by a client = the client is the sole data controller
- Researcher adds administration/contact information to sample file for researcher use only = agency is the sole data controller
- Researcher adds details of goneaways/deaths/do not select for future interviews = joint data controllers
- Researcher adds research data and respondent agrees to the information being attributed and shared with a client = joint data controllers.

VI. Data Processing

"Processing" means obtaining, recording or holding data or carrying out any operation or set of operations on the data including:

- the organisation, adaption or alteration of the data;
- retrieval, consultation or use of the data;
- disclosure of the data by transmission, dissemination or otherwise making available;

- alignment, blocking, erasure or destruction of the data.

VII. Sensitive Personal Data

This is defined as personal information covering:

- race or ethnic origin
- political opinions
- religious beliefs or beliefs of a similar nature
- trade union membership
- physical or mental health or condition
- sexual life
- the commission or alleged commission of an offence or any proceedings for an offence committed or alleged to be committed, or disposal of such proceedings or sentence of any court.

VIII. Consent

Data subjects must have a clear understanding of what will happen as a result of providing information (transparency). In the case of market research it can be assumed that this condition has been satisfied by the respondent agreeing to be interviewed following an explanation of the nature and objectives of the research. When undertaking market research the subject of the survey must be made clear, and if the respondent agrees to be interviewed and answers the questions, this is considered sufficient consent. When using a client sourced database or other third party sourced list as a sampling frame, the source of their personal data must be disclosed if a respondent requests this information. Also, this information can be disclosed at any appropriate point in the interview, rather than when the respondent requests it.

If conducting a survey, which incorporates sensitive personal data, the introductory text of the questionnaire should include sufficient information to ensure that the respondent is aware such information is to be requested. For example to describe a survey as covering "leisure activities" and to collect data about cinema attendance would be considered sufficient description to collect such data. However it would not be sufficient when collecting data about respondent's sexual activities – if this information were to be collected the respondent must be aware of this from the beginning of the survey.

Appendix 2

NOTIFICATION PROCEDURES

The full procedures are described within the MRS data protection guidelines, Appendix 1. The following notes contain the key points from this appendix.

Notification is the new term **replacing Registration**, for the process of informing the Information Commissioner of processing which is being conducted. Notification is a statutory requirement and replaces the previous responsibility for registration under the Data Protection Act 1984.

All organisations that process data must adhere to the Data Protection Act 1998 even if exempt from some or all of the data protection principles. Failing to notify activities to the OIC will not exclude individuals and organisations from adhering to the requirements of the Act.

Market researchers are not exempt from notification.

Organisations must notify with the OIC once a year. Notification currently costs £35 a year. To notify two forms (Part 1 and 2) must be completed and these ensure that general descriptions of the data held, the purposes and the recipients of the data are detailed for your organisation.

Notification must be completed directly with the OIC and this can be done by either printing off the notification forms from the OIC website (www.dataprotection.gov.uk) or by contacting the Notification helpline to request the forms. The Notification register is in the public domain and details can be checked via www.dpr.gov.uk

Detailed below is a guide on the forms and the kinds of information that will need to be detailed.

PART 1

Data controller – This should be the legal title of the individual or organisation. For example,

- Sole Trader – the full name of the individual e.g. Jane Catherine Doe
- Partnerships – the trading name of the partnership e.g. Doe & Co
- Limited or public limited companies – the full name of the company e.g. Doe Ltd
- Group of companies – these can not submit a single notification. Each data controller (each of the individual companies) must notify separately

Data controller address – For limited companies this is the registered address. For the remainder it should be the principal business address where the OIC can contact you.

Company registration number – The completion of this is optional.

Contact details – This does not appear on the public register but must be completed to allow the OIC to contact you.

A description of the processing of personal data – This is a general overview of the type of processing which is being conducted by your organisation.

For each purpose for processing you need to complete the following details,

PURPOSE: Most organisations will be processing data for a number of purposes and therefore each of these would need to be detailed with the data subjects, classes, recipients and transfers

detailed for each. A list of standard purposes and descriptions are provided. Whenever possible this should be used.

DATA SUBJECTS: These are the individuals about whom the personal data is held. A standard list is provided and this must be used.

DATA CLASSES: This is the type of personal data which is held about the data subjects. A standard list is provided and this must be used. It should be noted that within this list is all the 'sensitive' personal data classes. Most research agencies would be collected some if not all of these classes and this must be included on the notification form.

RECIPIENTS: These are the individuals to whom the data may be supplied. A standard list is provided and this must be used.

TRANSFER OF DATA: Within the Data Protection Act 1998 there are specific conditions which relate to data transfers outside of the European Economic Area (the EEA is all the countries in the EU plus Iceland, Liechtenstein and Norway). Therefore on the form you need to classify for each purpose whether the data is transferred world wide or only within the EEA.

Remember when you are completing this section that it will need to include not only details relating to your business e.g. research but also the details relating to the running of your organisation such as staff administration.

Once you have submitted details of the purposes you can add further purposes if the activities of your organisation expand during the notification year. This can be done by completing the purpose forms which are available on the OIC website.

The following is an example:

PURPOSE: Research

TYPE OF RESEARCH CARRIED OUT: Customer satisfaction surveys and new product development

DATA SUBJECTS: Customers

*DATA CLASSES: Personal details
Financial details
Racial or ethnic origin
Political opinions
Religious or other beliefs of a similar nature*

*RECIPIENTS: Employees and agents of the data controller
Other companies in the same group as the data controller
Data processors*

TRANSFER OF PERSONAL DATA: None outside the EEA

PART 2

Trading name - If trading under a different name from the formal legal title. This is for data subjects who may want to obtain details of the information held by you but are unaware of your organisation's full title.

Representative details – This is for data controllers who are not established in the UK or the EEA but are using equipment for data processing in the UK e.g. overseas market research organisations which have a CATI unit in the UK.

Security statement – A series of questions are asked regarding the measures you have in place to ensure that data is kept secure. These details are not shown on the public register.

Statement of exempt processing – There are a number of activities which are exempt from processing and this section is to make the OIC aware that not all your organisation's activities have been registered.

Voluntary notification – Organisations that are exempt from notification can do so voluntarily. The vast majority of market research organisations must notify so this would not apply.

If you were registered under the 1984 Act – This is for data controllers who may have had more than one registration under the previous 1984 registration regime. By completing this it will ensure that out of date entries will be removed.

Fees – Payment options for the £35 notification fee.

Declaration – This must be signed and dated.

Appendix 3

CATEGORISATION OF DATA COLLECTION PROJECTS

The rapid rise in the number of client organisations who hold databases containing details of their customers poses further issues within the 1998 Act for those undertaking research surveys. These issues cover:

- Providing feedback to clients where personal data drawn when sampling from a customer database are shown at the interview stage to be inaccurate or out-of-date;
- Enabling individual complaints or dissatisfactions about customer service raised by respondents during an interview to be fed back to clients at the respondent's request;
- Enabling clients to ensure that their customers are not "over-researched";
- Providing information back to clients that can be used to update data items other than personal details.

A new categorisation of projects has therefore been introduced to help members deal with these issues, and understand where the boundaries need to be drawn between "Classic" research and projects conducted for other purposes. These categories re-define the data collection processes used in the market research industry, and clarify the types and extent of feedback which can or cannot be undertaken or described as confidential market research as covered by the Code of Conduct.

Categories 1-5 cover projects which all meet the requirements within the definition of confidential market research. It is quite possible that a project may fit under more than one of these categories, depending on the source of the sample and the need to provide feedback of different types. The final category covers those projects that will not meet these requirements, due to some or all of the data being used for other than "Classic" research purposes. The following notes describe these categories in more detail:

Category 1: This category covers "Classic" confidential research with no feedback of any personal data unless to others involved in that specific project, provided they are already or have agreed to be bound by the MRS Code of Conduct and treat the data as for research purposes only (also, see Category 5, below). This would enable non-research specialists involved in a project to have access to individual respondent data.

An example: An architect is part of the research team conducting research into a housing project. The architect would need access to the raw data to aid in the analysis and interpretation. The architect would need to agree to the Code and other relevant legal issues (such as the Data Protection Act 1998) before they could be granted access to the data. The final research report will only report the data on an aggregate basis.

Category 2: This applies to research projects using samples drawn from client customer databases or other third party owned lists. In order to meet the fourth Principle in the 1998 Act agencies should notify the client of instances where the individual is either "no longer at this address" (but not of any new address) or has died.

An example: A charity client supplied a list of lapsed donors to a research agency. The charity wished to know why the individuals no longer contribute to the charity. As the charity had not had recent contact with many of the individuals the list contained a large number of 'gone aways' and individuals who have died. During the research project the interviewers marked on the database details of those who had died and those that had moved. The research agency passed these details to the charity to update their database; the agency did not supply any new address details for the gone aways.

Category 3: This also applies to the use of client owned customer databases for sampling. The agency provides back to the client the names, or list of identification numbers, of all those contacted solely for the purpose of setting up “do not select for research” (including those who declined to be interviewed on that occasion) markers on the customer database in order to prevent over researching individual customers.

An example: A supermarket supplied a list of loyalty cardholders to a research agency to conduct a customer satisfaction project. A number of individuals stated they did not wish to be contacted by the supermarket for research purposes. The research agency passed the relevant name and address details to the supermarket to update their ‘opt out’ flags on their database. This information was submitted separately from the research results.

Category 4: In this case a respondent, or the client, has requested that the interviewer(s) feed back to the client details of a specific complaint or dissatisfaction for investigation. The key points are firstly that the respondent must have given their consent – to both the principle of this feedback taking place and the content (to ensure that it accurately describes the details); secondly that the only details provided to the client are the respondents’ contact details plus a description of the complaint, and thirdly that the client can **only** use that information to deal with the issue raised and for no other purpose.

An example: A car manufacturer supplied a list of recent car buyers to a research agency to conduct a research project. During the research a number of individuals expressed extreme dissatisfaction with their new cars as a number of features were not working. When these issues arose the interviewers asked the respondents for their consent to pass the details to the manufacturer to enable them to resolve the problems. If the respondents consented the details of the problems together with the name and address of the relevant individuals were passed to the car manufacturer. The complaint information was submitted separately from the research results.

Category 5: In this case the client (probably the market research department) receives the results from the project at an individual respondent level but with the condition that the data at this personal level are only used for research purposes (as defined in the 1998 Act, see above, and the MRS Code). This responsibility must be part of the project contract between research agency and client. For projects where the research data is collected in the name of the research agency and not the client, consent to pass the data to the client must be gained from the respondent before it can be released. An example would be videotapes from group discussions.

An example: A telecom operator supplied a list of lapsed subscribers to a research agency to conduct a research project. The research department of the telecom client was keen to know the individual views of each of the sample and wished for the attributable comments to be passed to them with the aim to build a detailed research model. The research agency conducted the interviews on the basis that the attributable comments would be passed to the telecom operator for research purposes. Of the sample that responded 20% did not want their responses attributed to them. The research agency passed the attributable research results for the remaining 80% to the telecom operator having gained agreement from the client that the data will only be used for research purposes.

Category 6: This covers all projects where some or all of the data will be used by the client at a personal level for purposes in addition to or instead of those defined in the 1998 Act and the MRS Code as confidential research. These projects **must** conform to the MRS guidelines for collecting personal data for attributable purposes (Category 6 projects).

An example: A pharmaceutical company supplied a list of doctors to a qualitative agency to conduct some group discussions. In addition to the research the pharmaceutical company wants to be able to use the recordings from the group discussions for a salesman training conference to be held after the research. The agency briefed a qualitative recruiter to recruit the doctors highlighting the purposes of the recruitment (research and to produce training materials) and that the group discussions will be recorded with the intention of passing the details to the pharmaceutical organisation. At the group discussion the moderator reiterated the purposes, gains the consent of the respondents to the recording and to pass the recorded data to the pharmaceutical agency for research and training purposes. The research agency passed the

tapes of the group discussions to the client having gained written agreement from them that the data will only be used for the two specified purposes.

A key differentiation between Category 1-5 and Category 6 is whether the data from the project is used to understand and predict rather than take direct action directed at the individuals contacted.

Within all the above Categories, client organisations have the responsibility as data controllers under the 1998 Act to ensure that any data at a personal level passed back from an agency is used solely for the purpose(s) for which the respondent gave their informed consent. Agencies also need to ensure that their clients are conforming to the 1998 Act in respect of personal data passed to an agency to be used in a project (e.g. as a sampling frame). These responsibilities should be reflected in contractual relationships between clients and agencies.

Appendix 4

CLIENT ACTION PLAN (INCLUDING CONTRACT CHECKLIST)

The following provides a framework, or checklist, of key points to include within a client market research department data protection strategy:

- Read the advice and guidance available on the MRS (www.mrs.org.uk) & ESOMAR web-sites (www.ESOMAR.org). These sites are regularly updated on DP issues. Use MRS Codeline to resolve any outstanding queries.
- Identify the person responsible for covering data protection issues within the organisation and check that the data protection policy covers market research related issues. Ensure that any Notification covering any lists or databases that might be used for sampling purposes includes Market Research as a purpose. Check whether any 'opt-out' statements potentially restrict access to any customer records.

When reviewing a data protection policy check that the following information is covered:

- **The identity of the data controller:** the full legal title should always be provided. In cases where a trading name may be more familiar to the public than a legal title, both names should be provided. It is important that the same name as appears on the Information Commissioner's notification register is stated.
- **The intended purposes** the purposes must be described as fully as possible. Check that it sufficiently covers all market research and category 6 activities.
- **Opt outs:** legally market research does not need to be included as an opt out a data controller may want to include this.
- **Other information:** any non-obvious uses and data processing should also be included.

The BSI *Guide to the practical implementation of the Data Protection 1998* is a useful starting point in developing privacy policies and fair processing notices.

- If relevant, ensure that the guidelines for Category 6 type projects are applied.
- Write a data protection policy covering the market research departments activities for staff training and distribute/discuss with internal clients. Ensure this covers areas such as attending group discussions as observers, use of customer databases, feedback from projects (including the distinction between confidential market research and other purposes, database screening and cleansing, other feedback as described in the new Categories of data collection). Ensure that methodologies such as Mystery Shopping, Observation etc are covered, plus Category 6 projects – if relevant. Annually review the policy.
- Ensure contracts with agencies, data processors, fieldwork companies etc. adequately cover data protection issues, including identifying data controller responsibilities. Audit the data protection measures within third parties if necessary.
- The key points that need to be covered in contracts with agencies and other processors used in market research projects are as follows:
 - Use of data – restricting use to those specified in either party's data protection notification and notified to the data subject at the time of data collection. In addition it may be appropriate to restrict the use of the data to the data controller's purposes.
 - Destruction of data – detailing how the data should be handled once the contract has been completed or comes to an end.
 - Assistance with compliance – additional clauses may be added where data processors and data controllers provide appropriate assistance to meet each others data protection responsibilities (e.g. subject access requests, complaints, alleged breaches of the Act).

- Restriction on transfer of data – data can only be transferred outside of the EEA (which is the EU plus Liechtenstein, Norway and Iceland) where the receiver of the data has adequate data protection measures in place (see clause 1.9 for more detail) or where the respondent/data subject has consented to the transfer.
- Liability – this ensures that if a breach of the Act occurs in the completion of the contract a claim can be made for any loss incurred.
- Insurance cover – both parties should take out appropriate insurance to meet the liability for breach of contract.
- Security provisions - to ensure, that all hard copy and electronic address lists provided by the client are stored securely; destroyed; shredded; or returned to the client.
- Restrictions on the subsequent use of the data – e.g. the information supplied or collected during a project must not be used for future projects for other clients (i.e. to build respondent recruitment lists/databases).

(This list is not exhaustive and clients should refer to their own legal advisors for more information).

- Ensure that any transfers of personal data controlled by the company: between associated companies; to other companies/organisations; within Europe; outside the EEA; are compliant with the EU Directive. This may require seeking advice on the differences across the EEA in terms of national laws, and identifying those countries that the European authorities consider have adequate data protection legislation (see the UK Information Commissioners web-site www.dataprotection.gov.uk).

Appendix 5

DATA PROTECTION SCENARIOS

All the organizations, individuals and cases referred to in the following scenarios are fictitious

1. WEST BRACKENSHIRE DISTRICT COUNCIL

1.1 Scenario

West Brackenshire District Council has briefed Research UK to undertake a major telephone based satisfaction survey amongst local residents about the public services they provide within the District. The research will cover identified users of specific services, and general attitudes towards other services where users as such cannot be easily identified. WBDC will provide files from their residents' lists – these will be a mixture of individuals at private and business addresses.

The council has indicated their desire to re-interview certain types of respondents, but want to leave the definition of these until after they have seen the results of the survey. Research UK has call centres in several places across the UK, but decides that all interviewing will take place from the one located in Milton Keynes. As this is only about thirty miles away from the council offices, some of the managers have asked if it would be possible for them to come over to the call centre and listen in to some of the interviews as they take place.

Once interviewing starts, interviewers quickly discover that the lists seem to contain errors. Some residents are apparently no longer living at the address provided; some residents claim not to have used the service identified in the lists – and have asked the interviewers to ensure the council amend their files; some customers refuse to co-operate in the survey and say that the council has broken the data protection law by supplying their details to Research UK. Also, interviewers have encountered several dissatisfied residents who are asking interviewers to pass back to the council details of complaints that they claim have not been resolved.

Research UK calls the client to discuss these issues. The council decide to call a meeting with the agency to discuss the problems and asks them to collate details of each case to discuss in the meeting, after which WBDC intend to resolve them individually through the relevant departments. The council is also now asking for a data file containing the survey findings at individual respondent level.

1.2 Data protection issues

The data protection issues within this scenario are as follows.

This contains a wide variety of DP issues, and is complex due to the number of parties involved. Key points to consider are:

- There needs to be a detailed contract between the council and the agency covering the use of their data including data controller responsibilities, plus destruction & return of samples;
- If re-interviews are likely, then this needs to be built into the first interview. It would be better to ask all respondents;
- Listening to interviews needs to be for confidential survey research purposes only and these conversations should not be recorded in any way. Respondents would need to be advised and have consented. All this should be included in the contract;

- Assuming that the survey will be conducted in the name of WBDC, and then personalised results can be passed back to the client (Category 5), providing they are then used for market research purposes only – this needs to be included within the contract. However, in this case best practice might be to only provide WBDC with anonymised data;
- It is likely that Research UK will become a data controller for the personalised survey dataset. Overall, there will be joint data controller responsibilities for this project between client and agency;
- Whether West Barsetshire has Notified market research as a purpose;
- If asked, interviewers must provide respondents with the source of the contact details (i.e. the name of the council) at some point in the interview if a client provides the sample;
- Feedback on errors must be limited to 'goneaway' information **only** (Category 2), and, this must not include any new addresses. WBDC must not use this feedback to create a list of addresses for properties where residents no longer reside to use for other purposes. WBDC is the data controller and is responsible for keeping their databases up to date and error free, and this applies to **any** incorrect data items (e.g. incorrect information about service usage). The agency can indicate that there appear to be these other types of errors, but not the individual cases concerned;
- Complaints can be fed back as described in Category 4 – but WBDC must not use this information for any purpose other than resolving the complaints. The client needs to provide a contact point that will deal with these issues;
- The introduction to the interview needs to make it clear that this is a confidential survey research project and that any information provided to the client at a personalized level will only be used for market research purposes only;
- Those at the meeting must have agreed in advance not to use any personal information for any purpose that conflicts with the assurances given to respondents and must be in keeping with the 1998 Act and the MRS Code of Conduct. Categories 1, 2, 4.

2. EASTERN UNION BANK

2.1 Scenario

The Eastern Union Bank (EUB) has briefed Qualitative MR (QMR) to undertake a programme of group discussions about a proposed Internet banking service. QMR want to commission a fieldwork company to recruit respondents for the groups and hold the groups in centralized viewing facilities. The groups will be recruited from customer lists provided by Eastern Union Bank – these will contain private plus SME customers. EUB do not have a research department and the customer is one of the marketing team, who has indicated that those working on the project will attend the groups, and that they would also expect to have tapes of the groups to use within the bank. QMR have never worked with EUB before. EUB have specifically requested QMR not to identify the client.

2.2 Data protection issues

This is a typical qualitative project scenario. Key points are:

- Advising respondents about any recording of the proceedings when recruiting, and about the presence of observers;
- Bank customers may have been asked to opt in or out of activities such as marketing under the banking code of practice. Whilst there is no requirement to screen out these customers (apart from Category 6 projects), in certain types of research it might be beneficial in terms of customer goodwill to screen out such customers;

- Recruiters must be clearly briefed about returning/destroying sample data, and about not miss-using the information for other purposes (list building);
- The name of the client company must be disclosed at some point in the research process (recruitment or group discussion) if respondents request the source of contact details. It is also good practice if the observers are introduced to the group at some point in the session;
- Agencies should produce a guideline for those observing group discussions as best practice. This should include data protection issues, such as advising them that information they see or hear identifying individuals and their behaviour, attitudes etc is personal data covered by the 1998 Act and should be used for research purposes only;
- Wherever possible, clients' requests to have copies of/extracts from video/audio tapes should be resisted. If tapes are supplied then it is preferable if they are de-personalised – in any event, the client must understand (contractual clause) that they are provided solely for market research purposes. Usage in any other way (e.g. training sessions, sales conferences etc) would break the law (unless a Category 6 project). Transcripts should also be de-personalised;
- Particular care is needed in B2B qualitative research, as it is more likely that respondents can be recognized (perhaps by their opinions, voice etc) by client people when observing groups, viewing tapes or reading transcripts.
- Although the respondents are from the business sector their data would not be exempt from data protection legislation, as it is still personal data.