



& BMRA

Market research processes & the Data  
Protection Act 1998  
October 2002

## Foreword from the information Commissioner, Elizabeth France

“This guidance focuses on the key considerations for those carrying out Market Research activities on behalf of clients. It complements the comprehensive guidance already completed by the Society on the Data Protection Act 1998 and provides straightforward, practical advice. I commend the Society’s continued commitment to promoting high standards of compliance by its members.”

This material is provided for information only. It is not legal advice and should not be relied upon as such. Specific legal advice should be taken in relation to specific issues.

## 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](http://www.dataprotection.gov.uk)).

**There are eight data protection Principles within the Act and these form the fundamental basis of the legislation:**

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 2<sup>1</sup> of the Act is met, and
  - § in the case of sensitive personal data, at least one of the conditions in Schedule 3<sup>2</sup> 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

---

<sup>1</sup> 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,

- Ø the individual agrees to the processing
- Ø 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.
  -

<sup>2</sup> Schedule 3 of the first principle adds further conditions on processing if the data is “sensitive”. See Section C for full details.

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.

**The guiding principles of 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 data.

When collecting research data the purpose of the data collection must be transparent. Data collected only for market research purposes must only be used for that purpose. If data is to be collected for other purposes e.g. staff training this must be explained from the outset.

If a respondent's details are to be held on a 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.

## **SECTION B: 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 which 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.

### **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.

### **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 e.g. in the context of market research this may cover organisations that outsource fieldwork.

### **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.

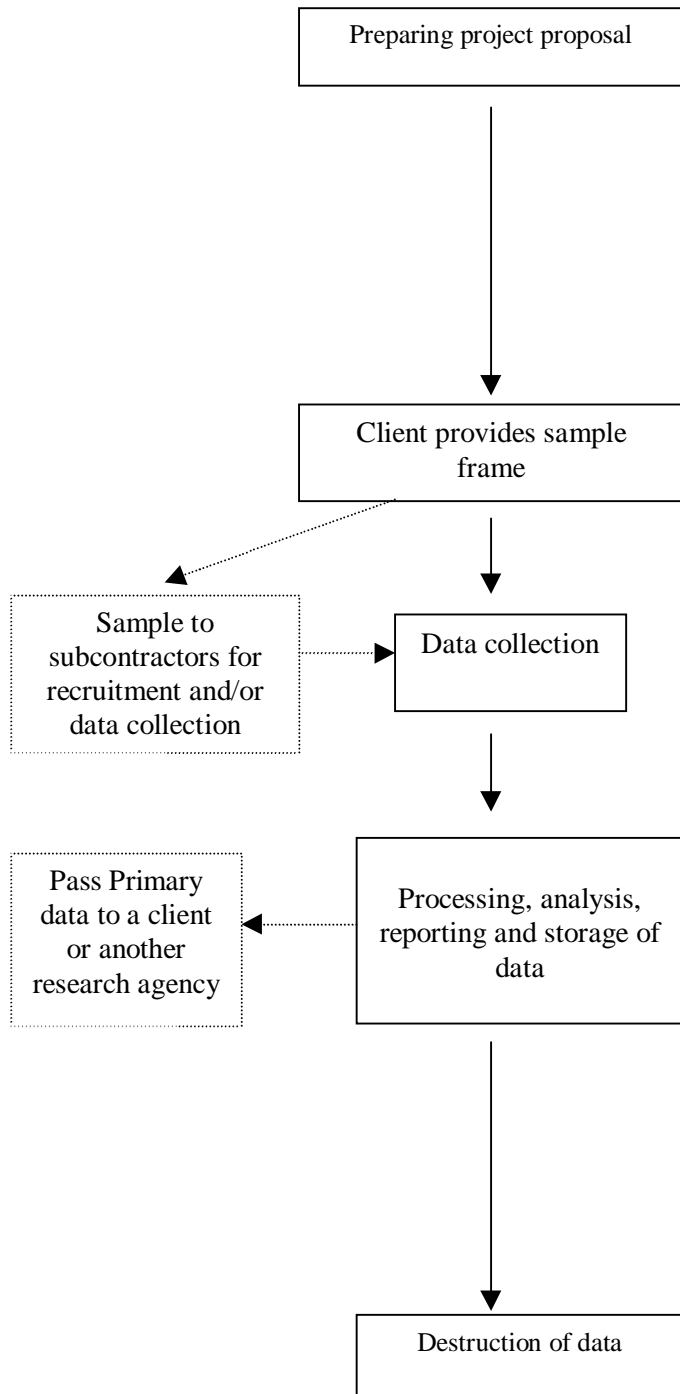
## **VIII. Consent**

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.

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.

## SECTION C: PROCESSES



### DPA Implications

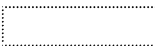
- 1.1 Contract & Data Ownership
- 1.2 Re-contacting Respondents
- 1.3 Anonymous Data
- 1.4 Third Parties
- 1.5 Client Identification
- 1.6 Transfer of Personal Data

- 2.1 Security
- 2.2 Data Screening
- 2.3 Sub-contractors

- 3.1 Qualitative Recruitment & Quantitative Interviewing
- 3.2 Security
- 3.3 Sample Cleansing
- 3.4 Interviewer Briefings
- 3.5 Observation Techniques

- 4.1 Security and Storage
- 4.2 Subject Access
- 4.3 Respondent Identification
- 4.4 Release of Primary Data

- 5.1 Disposal & Return of Data

 Activities in these boxes are only applicable in certain circumstances

## 1. PREPARING PROJECT PROPOSAL

At the time of preparing a project proposal 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 Contract & Data Ownership

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 notified with the Office of the Information Commissioner (OIC).
- § The notification must include 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](http://www.dpr.gov.uk)).
- § If additional data collection exercises are being conducted (such as direct marketing) the client must include this additional purpose in the Notification.
- § Market research organisations should check that the client is aware of their responsibilities under the UK Data Protection Act 1998.
- § Market research organisations must also “Notify” their activities with the OIC (see the Appendix in the publication *The Data Protection Act 1998 and Market Research: Guidance for MRS Members* for guidance on how to complete notification).
- § Market research organisations should include in their contract/terms and conditions their data protection responsibilities.

The contractual clauses covering data protection will vary depending upon whether the research organisation is either the data controller or the data processor.

### Data Processors

- § The Act requires that agreements with data processors be evidenced in writing.

### The following are some action points to consider if you are a data processor:

- § Prepare standard data protection clauses which you can suggest to a client as alternatives to client clauses which could be unnecessarily complex and difficult to understand.
- § Review existing contracts with subcontractors to ensure that any liabilities caused by their activities are passed on.
- § Choose subcontractors who can meet the data controller’s standards and not expose you to any liability.
- § Train staff and workers on their data protection responsibilities.

### Data Controllers

- § Data controllers should draw up **contracts** when releasing data to data processors.

## **The following are some action points to consider for inclusion:**

- § Security provision – stating the requirements of the Seventh Principle and that data processors need to comply with them.
- § 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 1.6 for more detail).
- § 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.

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

### **1.2 Re-contacting Respondents**

The Data Protection Act 1998 specifies a number of conditions which 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 to be held on a 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.

At the planning stage this restriction should be made clear to the client and a decision made whether to incorporate within the questionnaire.

### **1.3 Anonymous Data**

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 research organisation must assess with the client 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 with the consent of the respondent.

### **1.4 Third Parties**

Data can only be transferred to third parties, for their own use, once consent has been gained from the data subject. This is not applicable in instances where a client passes a sample frame to a research organisation on condition that the data is being passed for the completion of a contracted market research project only.

At the planning stage consideration should be given if the data is to be shared with more than one client and the appropriate permissions incorporated within the questionnaire to allow the data to be shared.

## 1.5 Client Identification

In instances where a client has supplied their own database for sampling the respondent has the right to know the source of the data if it is requested.

- § Market research organisations should make clients aware of this legal obligation if the client wishes to remain anonymous.

## 1.6 Transfer of Personal Data

**Any identifiable data sent outside of the EEA requires one of the following conditions:**

- § consent of the data subject;
- § contract with the receiver that they have adequate data security to meet the requirements of the Data Protection Act 1998;
- § the receiver signing up to the US “Safe Harbor” agreement (this applies to US companies only – see [www.export.gov/safeharbor/](http://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.

**Market research organisations should:**

- § agree with the client if the data is to be transferred
- § define where the data is to be transferred
- § include 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](http://www.europa.eu.int/comm/internal_market/en/dataprot/news/index.htm) for standard data protection clauses).

## 2. CLIENT PROVIDES SAMPLE FRAME

### 2.1 Security

The Seventh Data Protection Principle requires that where a data controller uses a data processor to process data on its behalf it must choose a contractor who can offer appropriate safeguards. This condition applies to all stages of the market research process including interviewing.

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. 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 market research organisations ensure that security is adequate to meet their client's and the Acts needs.

- § 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 receive data from a client to a market research organisation must be evidenced in writing.
- § Market research organisations should consider the following checklist regarding security when assessing whether their technical and organisation measures are appropriate:
  - § Are the automated systems protected by a level of security appropriate to the data held?
  - § Are technical measures in place to restrict access to systems holding personal data?
  - § Are technical measures in place to secure data during transit (e.g. to subcontractors and interviewers)?
  - § How is the data stored by your sub-contractors and interviewers – is it adequate and appropriate?
  - § Are the premises on which the data is held secure?
  - § Is access to the premises restricted?
  - § If the data is held on non-automated systems e.g. paper files, discs, microfilm, and microfiche, is access still restricted or secure?
  - § Are copies of printouts, obsolete back-up tapes etc disposed securely?
  - § Is obsolete hardware and software from which data could be recovered disposed of securely?
  - § Is there an auditable data retention and destruction policy?
  - § Are staff trained and made aware of their responsibilities to safeguard the personal data?

## **2.2 Data Screening**

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

- § The classification of data subjects to be included on a list supplied by the client.
- § Whether the list includes ex-directory numbers (for a telephone survey).
- § Ascertain when the list was last cleaned.
- § Any problems with the list.
- § Any pre-existing “opt outs” permissions that the client has must be reviewed. There is no legal requirement for market research to be included in the opt out permissions. However if a client has decided 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.

## 2.3 Sub-contractors

The requirement of ensuring personal data is held securely is also relevant when data is passed to sub-contractors. The security measures detailed in *section C clause 2.1* should be considered before passing data to sub-contractors.

## 3. DATA COLLECTION

### 3.1 Qualitative Recruitment & 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.

#### **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. Measures such as adopting encryption measures on CAPI machines should be considered.

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.

In instances 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.

### 3.2 Security

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.

#### **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: be stored securely; destroyed; shredded; or returned to the client.
- § **Questionnaires/documentation with identifiable respondent data:**
  - § These must be stored securely during use
  - § Questionnaires must never be handed to the client, either during or after an interview without the express permission of the respondent
  - § Where a research organisation is a data controller they must be aware of where documentation such as questionnaires are held. The respondent could ask for access to such information if it is in an identifiable format, and it would be incumbent on the research organisation to supply it.

### 3.3 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 should 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 (the Act does not cover those who have died and therefore this information can be fed back).

Details of incorrect data should 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 supplied by a client contains a high number of incorrect records the market research organisation should recommend that the client conduct a data cleansing exercise.

### 3.4 Interviewer Briefings

It is important that those who conduct the research (e.g. the interviewers) are aware of any data protection implications as a result of a data collection exercise.

**Listed below are a number of points to consider when drafting a briefing to interviewers:**

- § Source of the list – can the source of the list be revealed?
- § Client identification – does the client wish to remain anonymous? Are the interviewers aware of their requirement to reveal the source if the sample is from either a purchased list (e.g. from Dun & Bradstreet) or a client's database?
- § Identifiable data – is identifiable data to be passed back to a client? Is the interviewer aware of this to ensure they do not mislead the respondent during recruitment?
- § Incorrect data – does the interviewer know what they should do if incorrect data is found?
- § If telephone research – does the list contain ex-directory numbers? Has it been screened against the TPS?
- § Security of the data – are procedures in place to ensure the data is held securely whilst off-site?
- § Return of the data – are procedures in place to ensure the safe return of the data?

- § Recording of the interview – the interviewer will need to tell the respondent in advance if this is to take place. (In instances where recording is for **quality control purposes only** the respondent does not need to be informed although the interviewers must be informed.)

### **3.5 Observation Techniques**

In the case of observation studies, where no specific invitation to attend has been given, the research organisation must follow the CCTV Code of Practice produced by the OIC (for full details of the code see [www.dataprotection.gov.uk](http://www.dataprotection.gov.uk)).

#### **The main points from this code are:**

- § Recording equipment should be sited so that it only monitors areas intended for surveillance
- § Signs should state details of the individual/organisation responsible for the surveillance (including contact information) and its purpose
- § The quality of the recorded image should be appropriate to meet the purpose of the surveillance
- § Cameras should be situated in areas appropriate for the purpose of the surveillance
- § Images should not be retained for longer than is necessary
- § Disclosure of recorded images to third parties should only be made in limited and prescribed circumstances and with the individual's consent
- § Adequate security measures must be in place to ensure against any unauthorised processing, loss, destruction or damage of the data.

## **4. PROCESSING, ANALYSIS, REPORTING AND STORAGE OF DATA**

### **4.1 Security and Storage**

Once data collection has taken place the security of the data should be maintained (*as detailed in section C clause 3.2*).

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.

### **4.2 Subject Access**

When market research organisations hold respondent information in an identifiable format, the respondents have the right to see the personal data held about them. This relates to 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 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 a market research organisation 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.

Finally a small fee of no more than £10 may be charged by the data controller for the subject access request.

A subject access request does not have to be met if the results or any resulting statistics are not available in a form which identifies data subjects. While data is stored in an identifiable format respondents have the right of access to the data.

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.

Market research organisations may decide to remove all identifiers from their data. In such instances the organisation should formulate a policy on when and how the identifiable data is to be stripped away. It should be noted that if the data is to be anonymised this applies not only to the manual data and the current database, but also to any back-up records held.

### **4.3 Respondent Identification**

The identity of respondents and/or the use of attributable comments can only be used with the express permission of the respondent. Points to consider:

- § Questionnaire text must be clear when gaining permission from the respondents.
- § Information can only be used for market research purposes if it was on this basis that it was collected.
- § Respondents must not be harmed as a result of using data in this way.
- § Contracts with the client must contain clauses that restrict the client from using the data for purposes other than those stated at the time of data collection.

### **4.4 Release of Primary 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 C clause 1.6 for details*).

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 researcher and client.

## **5. DESTRUCTION OF DATA**

### **5.1 Disposal & Return of Data**

For quality standard purposes it is only necessary to keep primary data which is required for the analysis of the data and report preparation. Therefore for data which has been extracted during a research project (e.g. recruitment lists), which is not part of the data analysed for a project, the storage requirements do not apply.

All hard copy and electronic address lists must be held securely until destruction.

The research organisation should ensure that similar procedures are in place for any data held by sub-contractors involved in a project (e.g. interviewers and recruiters).

Research organisations should ensure that the destruction of the data is adequate for the confidentiality of the data being destroyed. For example any data which contains personal data should be confidentially shredded.