

**MRS/SRA**

**Data Protection Act 1998:  
Guidelines for social research**



**October 2005**

# CONTENTS

	<b>Page</b>
<b>Foreword</b>	<b>3</b>
<b>Acknowledgements</b>	<b>4</b>
<b>Introduction</b>	<b>5 - 7</b>
<b>Section A: Principles of the Data Protection Act 1998 (plus relationship with the Freedom of Information act)</b>	<b>8 -13</b>
<b>Section B: Research Project Processes</b>	<b>14 - 25</b>
<b>1. Commissioning</b>	
<b>2. Project Design &amp; Execution</b>	
<b>3. Processing, Analysis, Reporting &amp; Storage of Data</b>	
<b>4. Use of Data</b>	
<b>Appendix 1: Data Protection Act 1998 – Principles and Definitions</b>	<b>26</b>
<b>Appendix 2: Disclosure of personal data from research projects</b>	<b>27 - 29</b>
<b>Appendix 3: Data security</b>	<b>30</b>
<b>Appendix 4: Protocols to facilitate the sharing of personal data within the public sector</b>	<b>31 - 32</b>
<b>Appendix 5: Data Protection Scenarios</b>	<b>33 - 36</b>

## **FOREWORD**

*I welcome this guidance for social researchers produced by The Market Research Society (MRS) and the Social Research Association (SRA). I am keen to encourage representative bodies with an expert knowledge of a particular industry or activity to produce guidance for their members. Their practical knowledge is likely to ensure that guidance they produce focuses on the provisions of the Act which are most relevant in the context of the specific industry or activity concerned. This is certainly the case with this guidance. In particular I think that the MRS and SRA have made very good use of practical examples.*

**Richard Thomas,  
UK Information Commissioner**

## **ACKNOWLEDGEMENTS**

*These guidelines were produced as a result of a joint SRA and MRS working group.*

*We would like to thank all those involved particularly Peter Mouncey, MRS Fellow and member of the MRS Market Research Standards Board who completed a significant amount of the drafting of the guideline; and Roger Tarling, an SRA member and Mary Hickman, a member of the SRA Executive and Chair of the SRA Working Group on Dissemination, for their additional editorial support and for sharing their experiences of conducting social research.*

*We would also like to thank delegates who attended various SRA and MRS data protection seminars over the last two years. Many of the practical points included in the guidance are based upon real-life scenarios that delegates shared at these events. We recognise that only with the input and support of practitioners is it possible to develop guidance which is both accessible and practical to our members.*

*Ceridwen Roberts  
SRA Chairman*

*Debrah Harding  
MRS Deputy Director General*

## INTRODUCTION

The purpose of the following guideline is to provide advice and guidance on the Data Protection Act 1998 for those working in social research or others who commission social research projects.

During the whole of 2004, 60% of all queries received by the MRS Codeline service related to data protection. This illustrates just how important data protection has become in the everyday activities of researchers. In addition the new European wide Respect code of practice for social researchers includes a section referring to data protection issues.

The Data Protection Act 1998 is good for the 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;
- Research, as defined within the MRS Code of Conduct and SRA Ethical Code, continue to enjoy exemptions from certain aspects of the legislation. In addition, the market research sector 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 codes, 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 or regulators.

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

It is likely that most organisations either commissioning or conducting research projects 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. Where research is not a core activity, those responsible for data protection may not be fully aware of how the legislation impacts on this activity, or the important distinctions between research and other uses of personal data to support other activities. Some of these, such as those defined as direct or database marketing are more closely regulated by the 1998 Act. This guideline will therefore be helpful in ensuring that organisations make the right decisions when commissioning 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 below).**

The following 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'*, and also complements a further guideline on how the 1998 Act impacts upon research agency processes *'Market Research Processes and the Data Protection Act (DPA) 1998'* produced by the MRS and the BMRA and the Client Data Protection Processes Guidelines produced by the MRS and Aura . For full details of all these guidelines see [www.mrs.org.uk](http://www.mrs.org.uk). **Also, specific industries may have guidelines and interpretations of the Data Protection Act 1998 that may apply to research (e.g. the banking and**

**pharmaceuticals industries – see the Code/Guideline section of the MRS website for more details).**

The following points may help researchers understand the key points of how the Data Protection Act 1998 (DPA 98) relates to their work:

- If you undertake research that uses or collects personal information about identifiable, living people then you will need to comply with the DPA 98;
- The Act applies to any research that uses or gathers personal data – qualitative, quantitative; electronically or manually held, apart from data already in the public domain;
- The Act only applies to data that identifies a living individual, therefore as soon as personal identifiers are removed from the research data the legislation no longer applies;
- The Act lists types of personal data that under certain legal circumstances must be made available to the public;
- In the majority of cases, samples used for confidential research purposes do not need to be pre-screened against the Telephone, Mail and Fax Preference Services but any 'do not contact for research purposes' markers must be respected;
- Ensure that a potential respondent has a very clear and unambiguous understanding of the purpose(s) for collecting their personal data and how it will be used ('transparency');
- Ensure that respondents have given their consent to their data being collected, and also at that time, have been given the opportunity to opt out of any subsequent uses of the data ('informed consent');
- Data collected for one purpose cannot be subsequently used for a different purpose unless the individual has given their permission ('You can change the rules, but not after the game has been played' – Howard Beales, Federal Trade Commission);
- In most cases you must obtain permission to re-interview at the time of the first interview;
- Personal data collected in the name of the researcher can only be transferred to the client, even if for research purposes, with the explicit consent of the individual respondent;
- If they ask, respondents have the right to know the source of any personal data used to recruit them;
- Make sure that interviewers return or destroy any sample sent to them and ensure they do not use the information to create their own recruitment lists;
- Tell respondents for groups when you recruit them whether the groups will be recorded or are to be observed (by the client);
- Check that you have clearly identified the data controller responsibilities for yourself (your organisation) and the client;
- Where you use a sample provided by the client, or other third party, check on the Information Commissioners web site that your client has appropriately notified the purpose(s) and disclosures for their personal data;
- Check that your own organisation has notified and that the notification is adequate. Your organisation may have appointed someone to look after data privacy issues who can help;
- Written contracts with data processors are mandatory, but it is also advisable to have written contracts in place with clients.

Finally, when thinking about the potential data protection implications within a particular research project, take a common sense perspective and put yourself in the respondent's shoes. If you think that a respondent in a research project might be surprised by any subsequent use you make of their personal data, then there is a chance that you have not met

the requirements of the Data Protection Act 1998 or the interpretation of this legislation in the context of social research, as described within this guideline. For example:

- re-contacting a respondent for follow-up research without having raised the possibility and asking for their consent to do so during the initial contact;
- transferring a respondent's personal data to a researcher other than the one(s) in whose name it was collected in the first place without have gained the respondent's consent during the initial research/data collection;
- Using a quotation from a research interview in a report which might be easily attributed by a reader to a particular respondent without having gained their prior permission.

### **Definitions used in the guideline applying to research**

Within this guideline, the following definitions are used for 'Researcher', 'Client and 'Research':

#### **Researcher**

'Researcher' includes any individual, organisation, department or division, including any belonging to the same organisation as the client which is responsible for, or acts as, a supplier on all or part of a research project.

#### **Client**

'Client' includes any individual, organisation, department or division, including any belonging to the same organisation as the researcher, which is responsible for commissioning or applying the results from a research project.

#### **Research**

Research is the collection and analysis of data from a sample of individuals or organisations relating to their characteristics, behaviour, attitudes, opinions or possessions. It includes all forms of market, opinion and social research such as consumer and industrial/business to business surveys, psychological investigations, qualitative and group discussions, observational, ethnographic and panel/longitudinal studies. It includes quantitative and qualitative methodologies.

'Confidential survey research' must only be used to describe research projects which do not disclose personal details at an identifiable level.

## 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)).

Appendix 1 summarises the key Principles within the 1998 Act.

### ***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 data<sup>1</sup>.

When collecting research data the purpose of the data collection must be transparent. Data collected solely for **confidential 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.

If a respondent's details are to be *kept* on a client or researcher 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. However, this excludes follow-up interviews conducted solely for quality control purposes ('back-checking')

To help researchers and their clients understand how the 1998 Act and the MRS Code of Conduct affects the permissible flow of personal level data from research projects, the industry has developed a detailed description of permitted disclosures and associated conditions applicable to research projects. These categories are summarised within Appendix 2.

### **Key definitions**

The following list describes the key terms used within the legislation relevant to social research:

#### **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 length of employment. The Act also covers personal data held on media such as video/audio tapes, CCTV and digital formats.

Once the personal identifiers have been removed from the data then the resulting anonymised dataset is no longer subject to the Act. Therefore, the sooner the identifiers are removed the sooner the data will no longer be subject to the Act. The latest version of the MRS Code of Conduct no longer includes any recommended period to keep primary data records – this is for the researcher to decide based on the type of research, other legal requirements, contracts with clients or internal administration needs.

---

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

At the planning stage the researcher 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 research exercise on the condition that it is used only for the purpose for which it was collected (e.g. research purposes) and with the consent of the respondent.

### Consent

Data subjects must have a clear understanding of what will happen as a result of providing information (transparency). In the case of 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 research the subject of the research 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.

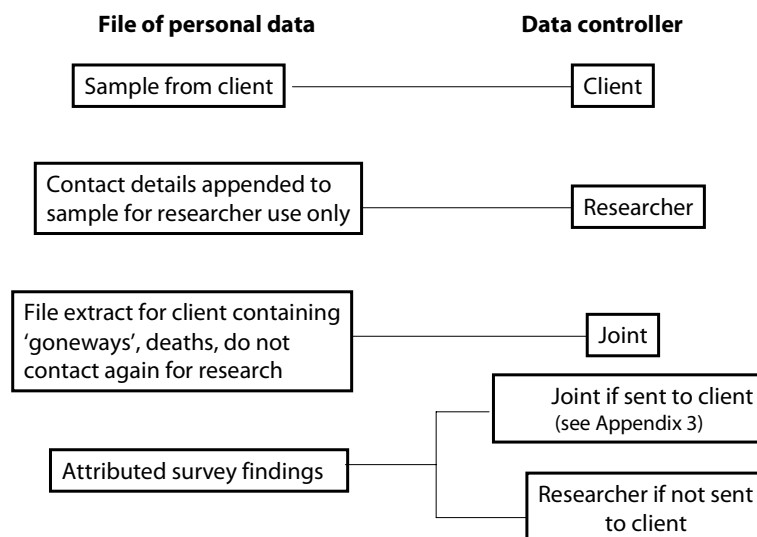
If conducting a project, which involves collecting sensitive personal data, the introductory text of the questionnaire should include sufficient information to ensure that the respondent is aware such information is to be requested. For example to describe a research project as covering "leisure activities" and to collect data about usage of the local swimming pool 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 interview.

There is no requirement for researchers to gain prior consent from potential respondents before the interview, even where sensitive data will be collected.

### 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). The following diagram describes the data controller responsibilities between a client and the researcher:

#### Defining data controller responsibilities



Also, see Appendix 3 for the data security issues that Data Controllers need to consider.

## 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.

Also see Appendix 3.

## Data Processors (also see Appendix 3)

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 research this may cover organisations that undertake fieldwork only or data processing).

It is unlikely that a researcher 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 researcher uses this as a master file for the projects. Clients and researchers working on their behalf may therefore both become separate data controllers for databases containing some of the same data. Similarly clients and researchers may be joint data controllers for data sets that are shared between two parties (e.g. with some panel data). See the diagram under **Data Controllers**, above.

## Data Subject

The data subject is the **living, natural, 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. Sole traders and partnerships are also categorised as data subjects in England and Wales and sole traders are data subjects in Scotland. Other types of organisations are exempt. Some further points:

- Once someone has died, information about them is no longer subject to the Act;
- Children have the same rights as adults;
- Personal data about sole traders or partners in a partnership (e.g. solicitors practice) count as data subjects;
- Data about an employee’s job will not usually constitute personal data.

## Manual Data

The Court of Appeal has ruled that the only personal data held in manual files covered by the DPA98 is that which is held in a ‘relevant filing system’ – the Act is intended to cover manual files ‘only if they are of sufficient sophistication to provide the same or similar ready accessibility as a computerised filing system’. Any manual filing system which requires the searcher to leaf through files to see what and whether information qualifying as personal data of the person making a Subject Access request is to be found there and would bear no resemblance to a computerised search is unlikely to qualify as a ‘relevant filing system’.

One ‘rule of thumb’ suggested by the Information Commissioner is the temp test: If you employed a temporary administrative assistant would they be able to extract specific

information about an individual without any particular knowledge of your type of work or the documents you hold. If the answer is 'yes' then the files are probably covered by the DPA98

## **Personal Data**

'Personal data' has recently been defined by the Court of Appeal<sup>2</sup> as:

'information that affects (a person's) privacy, whether in his personal or family life, business or professional capacity. 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.

Data about employees that simply describes their role within an organisation, or where the data is related to the role rather than the individual is not classified as personal data. So, if a research project of IT directors was only collecting data about the responsibilities of IT directors and the interview solely covered aspects of the organisations IT procurement policies, then the data would be unlikely to be categorised as personal data. However, if the questions included attitudes of the respondent, and a full demographic profile of each individual then the data would be personal data.

## **Notification**

'Notification' is the process replacing the 'Registration' required within the earlier data protection legislation (1984) 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.

It is a statutory requirement under the 1998 Act and all data controllers need to ensure that all relevant activities involving the use of personal data are notified to the OIC using the forms (Part 1 and 2) available either on their web site ([www.informationcommissioner.gov.uk](http://www.informationcommissioner.gov.uk)) or via the OIC helpline. Data controllers must notify annually. All notifications are in the public domain (see [www.dpr.gov.uk](http://www.dpr.gov.uk)).

Any client, or researcher, owned databases containing details of customers, patients, employees, tax payers, personal level research results etc would need to be notified, and, if they are to be used for deriving research samples, then the entry on the register needs to include research as a purpose for which the data will be used. Data controllers have the option to add a further description to this purpose e.g. customer satisfaction research.

Social research activities are **not** exempt from notification.

## **Sensitive data**

This is defined as personal information covering:

- race or ethnic origin
- political opinions
- religious beliefs or beliefs of a similar nature

---

<sup>2</sup> Micheal John Durant v Financial Services Authority [2003] EWCA Civ 1746, Court of Appeal (Civil Division) , 8<sup>th</sup> December 2003.

- 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.

The 1998 Act contains specific rules covering the collection and use of 'sensitive' data. In particular, the Act requires data collectors to ensure that they have gained the 'explicit' consent of the data subject prior to collecting sensitive data. In terms of research interviews, then as long as the key rules of transparency and consent, as described above, have been observed, then by agreeing to be interviewed the principle of 'explicit' consent has been satisfied.

***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 a description of the Notification procedures.***

### **Relationship between the Data Protection Act (DPA) the Freedom of Information Act (Fol)**

The Fol creates a right of access to official information and places a duty on public authorities to publish information. The act became law on the 1<sup>st</sup> January 2005. However, whilst the Information Commission is the regulator for the data protection act within England, Wales and Scotland, the IC's powers covering the Fol act only apply to England and Wales, there being a Scottish Information Commissioner responsible for the Fol within Scotland. The difference between the Freedom of Information Act (Fol) and Data Protection (DPA) is that the DPA enables individuals to gain information about themselves whereas the Fol enables individuals to gain information about public authorities. Research data and research projects are not exempt from the Fol, but personal level data may be exempt under the act and as such this legislation cannot be used to gather personal data about individuals such personal data should only be released if this would not breach requirements of the DPA. Also, research project related data and information might be exempted where it is judged by a public body, using a prescribed test process, to be in the public interest to do so (e.g. commercially sensitive information). This decision must be justified. The Scottish Executive, for example, require those responding to invitations to tender to place commercially sensitive information into an annex plus a description of the harm that might result from disclosure or publication. Some public data, collected for example in statutory business research or the Census are protected by other legislation.

Examples of research project information that might normally be made available include:

- Invitations to tender
- Unsuccessful tenders & assessments of them (with commercially sensitive information removed)
- Details of the successful tender including pricing (with commercially sensitive information removed)
- Details of how the project is managed, progress reports and reports on contract management
- Questionnaire
- Reports based on the research
- Existing data that is available but not published in reports (there is no obligation to generate new information, for example from further analysis, to meet a request). This can be provided in a summarised form.

Information is only available via a public body.

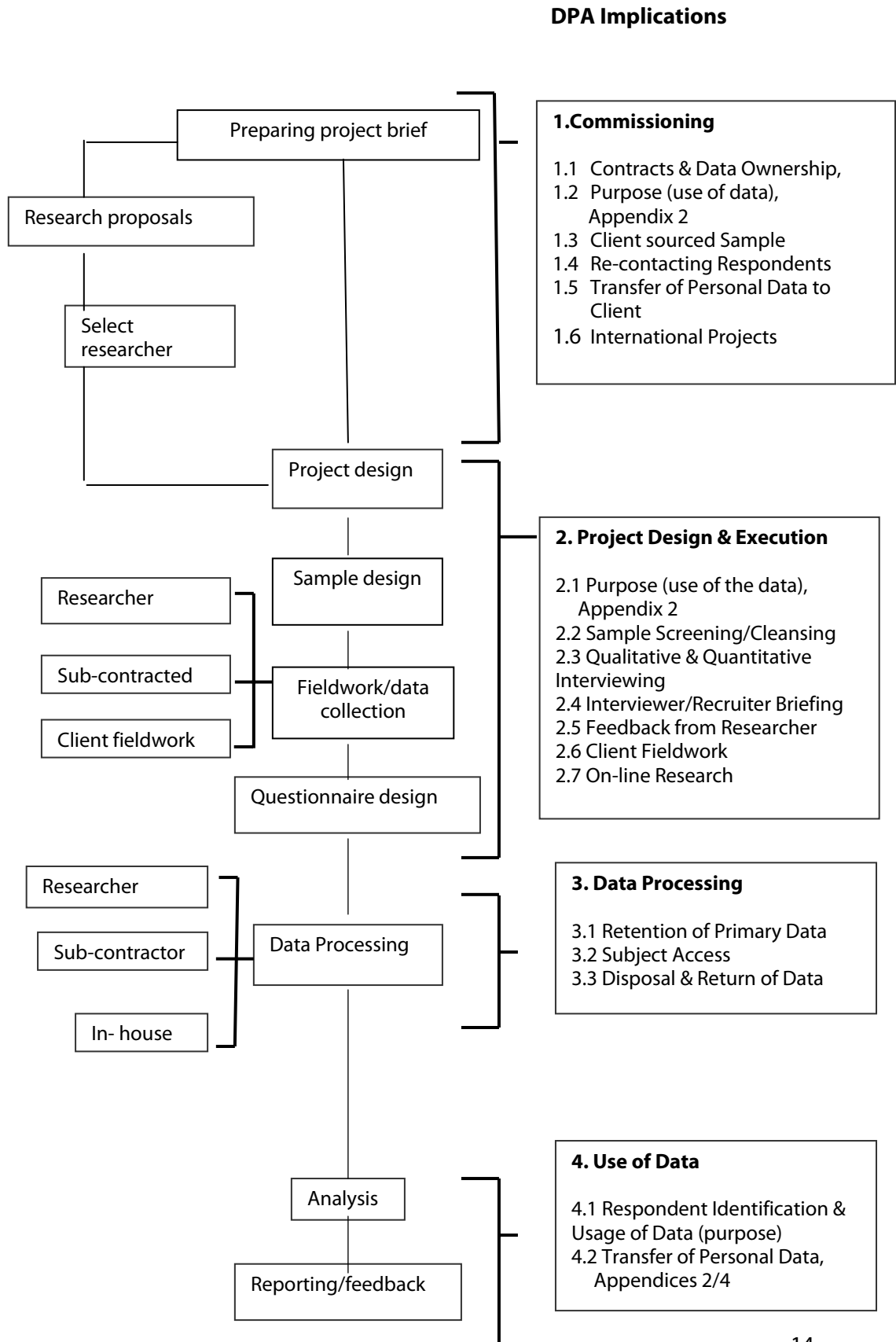
Data that is of poor quality, from flawed methodologies or is not considered 'fit for purpose' would not normally be exempt.

Further information on the FoI for England and Wales is included on the Information Commissioner's web site, and for Scotland see [www.itspublicknowledge.info/index.htm](http://www.itspublicknowledge.info/index.htm) and [www.scotland.gov.uk/socialresearch](http://www.scotland.gov.uk/socialresearch) (the Chief Researcher in the Office of the Permanent Secretary, Analytical Services Group within the Scottish Executive issued advice on the implications for social research projects in April 2005).

## 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 Research Process



## 1. COMMISSIONING

At the time of preparing a project brief and reviewing researcher 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

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 a researcher 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 commissioning research. When the client supplies data for sampling purposes the following conditions apply:

- The client must have completed their annual notification with the Office of the Information Commissioner (OIC) – this can also be checked on [www.dpr.co.uk](http://www.dpr.co.uk).
- 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.informationcommissioner.gov.uk/eventual.aspx?id=3](http://www.informationcommissioner.gov.uk/eventual.aspx?id=3)).
- If the project includes data collection for purposes other than purely for research the client must include this additional purpose(s) in the Notification.
- Clients should check that the researcher 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. local authority Council tax payers, NHS hospital trust patients 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 respondent contact and profile details supplied by the client plus research findings. They need to ensure that this is clearly defined and reflected within the contract.
- 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 researcher 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 research data at a personal level is to be shared with more than one client and the appropriate explicit permissions incorporated within the questionnaire to allow the data to be shared.

- Conditions for transfer are actually very limited and specific. There are certain protocols, or legislation, covering the public sector that enables personal data held within one public body, or elsewhere, to be shared with another public body. One or more of these may apply to sharing or disclosing personal data for research sampling purposes. See Appendix 4 for further details.

See Appendix 3 for Data Security issues.

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

## **1.2 Purpose (use of personal data)**

Clients should clearly state within the brief if they require the researcher to provide them with personal data collected within the project and describe any purposes other than research that this data will be used for (see Appendix 2).

## **1.3 Client Sourced Sample**

It should be noted that any breach of the Act that occurs while personal data is held by a researcher, 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 researcher would result in the owner of the data (the client) paying the compensation. Therefore it is essential that clients check that researchers have adequate security processes to meet clients' and the Act's needs and that the contractor has understood and accepted their responsibility. A data controller can not by contract evade liability under the DPA.

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 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 about the issued sample is required by the client or personal level data then this should be specified (see Appendix 2 for disclosure rules).
- If the personal data from the research is to be used for any purpose other than research then the sample file will need to be screened against any appropriate lists such the Mail and Telephone Preference Services files or to respect any relevant 'do not contact' markers on the client file.
- 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.

- Researchers must provide adequate 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 researcher must be evidenced in writing.
- The researcher needs to agree with the client how to respond if any respondents drawn from a client supplied list query the right to transfer their details to a researcher to use for research purposes. The client Notification covering the source must include research.
- Care should be taken if known ex-directory numbers are to be included in a telephone research project; any relevant opt-outs should be respected (e.g. a marker on the file stating that the individual does not wish to be contacted for social, market or research purposes – also see Appendix 2). 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.
- If one or more separate client organisations or legal entities (for example, different hospital trusts, local councils, companies within a group or universities etc) are planning a joint research project using samples drawn from their respective databases, then personal data about respondents cannot be shared across these entities without the consent of respondents or unless a data sharing agreement is in place which has been approved by the appropriate government departments. This only applies to attributable data. It is therefore preferable if the merging is undertaken by a researcher.

#### **1.4 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) to do with this topic (or where information collected in this first interview could result in them being re-selected 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. Care should be taken to ensure that ‘soft’ refusals (e.g. ‘I’m busy now, could you call later?’) can be clearly differentiated from ‘hard’ refusals (e.g. ‘I don’t want to be interviewed’) when identifying legitimate call-back situations.

#### **1.5 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. a fifty year old widow with a medical exemption certificate).

At the planning stage:

- The client needs to decide whether the project will be conducted in the name of a third party (i.e. a researcher) rather than the name of the client. Identifiable data can be collected and passed to a client during a research exercise on the condition that it is used only for the purpose for which it was collected (e.g. research purposes), and, if the data is collected under the name of the researcher the respondent must have been given a clear expectation that their data at a personal level will be transferred to the (named) client, and been given the opportunity to prevent this (‘opt-out’). (see Appendix 2 & 4 about disclosures).

## 1.6 International Projects

Any identifiable data sent outside of the European Economic Area (EEA) (the countries subject to the Directive on data privacy), other than for purely data processing purposes, requires one of the following conditions<sup>3</sup>:

- 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/](http://www.export.gov/safeharbor/) for more details).
- The researcher and client 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 researcher 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](http://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 conducted amongst them. Similarly, if an organisation 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 research projects need to include a clear statement of the purpose (i.e. ‘research’, and what this means in terms of protecting the identity of the respondent).

For projects conducted for a purpose in addition to research, the questionnaire must include a statement that describes all purposes that the data will be used for. Respondents must also be given the opportunity to state if they do not wish their personal data to be used for any proposed purpose and have this wish respected (‘opt-out’).

### 2.2 Sample Screening/Cleansing

---

<sup>3</sup> The International Chamber of Commerce is currently developing new rules for transferring data to countries outside the EEA (November 2004)

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

- The types of data subjects (e.g. business or private individual; adults or children etc) included on lists supplied by the client
- Use of personal data held by other divisions within an organisation, or subsidiaries, (e.g. a customer sample drawn from multi-sources) requires the prior permission of the data subjects concerned if any of the sample sources are to be used for research purposes.
- Whether the data controller/s Notification includes research as a purpose.
- Whether the list includes ex-directory numbers for a telephone research project (see 1.3 for further guidance).
- Ascertain when the source list was last cleaned.
- Any known problems with the source list.
- Any pre-existing “opt-out” permissions that are present in the file must be reviewed. There is no legal requirement for research to be included in the opt-out permissions. However if a client decides to include 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 research must be screened out of the sample provided to the researcher.
- There is no legal requirement to screen research samples against the preferences services (such as the Telephone Preference Service) when conducting 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 conducted for direct marketing purposes 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 researcher 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 researcher or the client. (For example one approach could be providing the information in the preamble to a research project: ‘Good morning, I am working for XYZ research company on behalf of ABC Hospital Trust. We are conducting a market research survey about your attitudes as an out patient of ABC Hospital Trust.....’).
- During the recruitment process for *qualitative* research projects:
  - 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 if 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. Researchers 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 at the start of the interview, 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 or at any appropriate earlier point in the interview.
- 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 eliminated from the final analysis and reporting.
- Any people observing a group must be made aware that the content of the discussion counts as 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 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 guidelines covering attributable research projects (see Appendix 2 and MRS web site).
- If a subject access request is received for recorded data the information can be supplied in alternative formats (such as a transcript) in order to protect the identity of other respondents (unless all those included in the recording have given their consent for the recorded information to be released).

In the case of observation studies, where no specific invitation to attend has been given, the researcher 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)).

#### **2.4 Interviewer/Recruiter Briefing**

The DPA 98 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:

- All hard copy and electronic address lists must be stored securely during use and destroyed; shredded; or returned to the client/third party after use as required. 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.
- Completed, or partly completed questionnaires, which include personal data which could identify respondents, must **never** be shown to the client, either during or after an interview without the express permission of the respondent.

## 2.5 Feedback from Researchers (inc Sample Cleansing)

If a supplied list contains incorrect information, for example an incorrect address or telephone number, then the fact that this information is inaccurate must be fed back to the client. However, as the client (or other third party) is the data controller for the list and responsible in law for keeping it accurate and up to date, any *corrected* data (e.g. a new address) cannot be supplied back to the client without the express permission of the individual concerned – otherwise, the client needs to source and verify any necessary corrections. Circumstances may arise where a researcher does identify a change of address and this information may be passed back to the client. It is still the responsibility of the data controller to ensure that this information is correct before updating their database. The Act does not cover those who have died and therefore this information can be fed back.

- 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 research project should not be used for other purposes (e.g. cannot be used by utility companies to target new home owners to switch suppliers).
- 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 researcher separately from the research findings. The information must not be used for any other purpose.

See Appendix 2 for full details of the disclosure rules.

## 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’. In particular, 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 (see 1.5, above)? 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?
- 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**, such as in telephone interviewing, the respondent does not need to be informed although the interviewers must be informed.)

## 2.7 On-line Research

If a client undertakes its own on-line research, then the web sites must contain sufficient information regarding their 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 and social 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 researcher should agree a data security, retention and destruction policy within the original contract and these conditions must be met.

For example, for an ad hoc project it may be possible to destroy the personal data three months after the project has been completed; for a respondent who is no longer on a continuous panel, then the period may need to be longer. The latest version of the MRS Code of Conduct no longer includes any recommended period to keep primary data records – this is for the researcher to decide based on the type of research, other legal requirements, contracts with clients or internal administration needs.

### 3.2 Subject Access

When clients or their researchers hold respondent information in an identifiable format (e.g. client supplied lists held by a researcher used as sampling frames, completed questionnaires etc) the respondents have the right to see the personal data held about them. This includes any data held on computer files, certain forms of 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". However, only data controllers have the right to deal with subject access requests. Therefore, a subject access request received by a researcher can only be met for data where the researcher holds sole or joint data controller responsibility. So, if the request covers information provided by a client for which they are the data controller to a researcher then only the client can deal with the request (e.g. the sample file provided by the client). 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. Therefore, those undertaking confidential research projects should separate identifiers from the research data as soon as is practical to do so, and not retain primary data collection material (e.g. paper questionnaires) longer than is necessary (also see 3.1, above).

- If a subject access request is received a client or their researchers may have to comply and provide copies of all identifiable data held about a respondent. If subject access requests fall within the rules but would be of a disproportionate effort and costly to fulfil in a permanent format for either the researcher or the client they still have to provide access under the Act 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).
- Subject access requests need only be met if 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 be charged by the data controller for the subject access request. It is at the discretion of the Data controller if a fee is charged and this should form part of a client's and/or researcher 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 (also see Appendix 3)

The contract with the researcher (and with any data processors) 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, or other personal data, must be held securely by the researcher until either these are returned to the client or destroyed by the researcher.
- Clients should check that the researcher 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 be sufficiently clear to ensure there is 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 (see Appendix 2). In particular, data collected for 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 hospital out patient’s 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 hospital).
- Care must be taken if data from a research project is used to develop models to ensure that individual respondents cannot be identified. For example, it could be possible to identify an individual respondent 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 illness profile 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 1.6 for details*).
- Transfers of personal data (e.g. customer data) from one legal entity to another within the same overall organisations, or group of organisations, may require prior permission from the individuals concerned. Within the public sector there are protocols and other legislation that have been developed to facilitate the sharing of personal data. These are described within Appendix 4
- For audio, video recordings or transcripts to the client:

- All individuals concerned must have consented to the subsequent release of the data to the third party and the purpose(s) to which the data 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

These conditions should be stated in the contract between the client and the researcher.

## Appendix 1

### DATA PROTECTION ACT 1998: 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 2<sup>4</sup> of the Act is met, and
  - in the case of sensitive personal data, at least one of the conditions in Schedule 3<sup>5</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
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.

---

<sup>4</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,

- 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.

<sup>5</sup> Schedule 3 of the first principle adds further conditions on processing if the data is "sensitive". See Section B for full details.

## Appendix 2

### DISCLOSING PERSONAL DATA FROM RESEARCH PROJECTS

The rapid rise in the number of research projects where the samples are drawn from databases (e.g. citizens, customers, employees, patients, offenders etc) poses issues to do with the disclosure of personal data within the 1998 Act.

The following types of disclosure are all permissible within projects described as research:

1. Where there is a need to disclose personal data to people working on a project who would not normally be described as researchers and covered by an existing code such as the MRS Code of Conduct. The individuals concerned would need to have agreed to abide by the principles contained within such codes and thereby ensure that the data was not used for any other purpose. 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.*

2. Where research projects use samples drawn from client databases or other third party owned lists, agencies should notify the client/third party (data controller) of instances where when attempting to interview an individual they are either “no longer at this address” (but not of any new address) or has died in order to meet the fourth Principle in the 1998 Act.

*An example: A charity client supplied a list of lapsed donors to a researcher. 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 ‘goneaways’ 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 researcher passed these details to the charity to update their database; the researcher did not supply any new address details for the gone aways.*

3. Where a client database has been used for sampling purposes, the researcher can provide the client with 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 university supplied a list of recent l graduates to a researcher to conduct a student satisfaction project. A number of individuals stated they did not wish to be contacted by the university for research purposes. The researcher passed the relevant name and address details to the university to update their ‘opt out’ flags on their database. This information was submitted separately from the research results.*

4. Where 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. This information must be provided totally separated from the research results for that individual.

*An example: A housing trust supplied a list of tenants in new properties to a researcher to conduct a research project. During the research a number of individuals expressed extreme dissatisfaction with their accommodation 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 housing trust 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 housing trust. The complaint information was submitted separately from the research results.*

5. A client (probably the research department) can receive 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. This responsibility must be part of the project contract between research researcher and client. For projects where the research data is collected in the name of the researcher and not the client, consent to pass the data to the client must be gained from the respondent before it can be released. Simply naming the client would not be sufficient – respondents must be left with a clear expectation that their data will be shared with the client. An 'opt-out' maybe necessary in certain circumstances (see the detailed example below) An example would be videotapes from group discussions.

*An example: An NHS hospital trust supplied a list of outpatients to a researcher to be used in a research project. The research department of the NHS trust 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 researcher conducted the interviews on the basis that the attributable comments would be passed to the NHS trust for research purposes. Of the sample that responded 20% did not want their responses attributed to them. The researcher passed the attributable research results for the remaining 80% to the NHS trust having gained agreement from the client that the data will only be used for research purposes.*

6. Disclosure to clients of personal level data is also permissible for projects where some or all of the research results at a personal level will be used by the client 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, *Using research techniques for non-research purposes (currently in draft format)*. Where this type of disclosure will take place, the interview **must not** leave the respondent with the impression that they are taking part in a confidential research project.

*An example: A pharmaceutical company supplied a list of doctors to a qualitative researcher 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 researcher 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, gained the consent of the respondents to the recording and to pass the recorded data to the pharmaceutical researcher for research and training purposes. The researcher 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 disclosures within research projects and other disclosures from other types of 'research' is whether the data from the project is used to understand and predict rather than take direct action directed at the individuals contacted.

***Client organisations have the responsibility as data controllers under the 1998 Act to ensure that any data at a personal level passed back from a researcher is used solely for the purpose(s) for which the respondent gave their informed consent. Researchers also need to ensure that their clients are conforming to the 1998 Act in respect of personal data passed to a researcher to be used in a project (e.g. as a sampling frame). These responsibilities should be reflected in contractual relationships between clients and researchers.***

## Appendix 3

### Data 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 research process including interviewing.

It should be noted that any breach of the Act that occurs while personal data is held by a researcher, on the client's behalf, e.g. a list supplied by a client for sampling purposes, could result in the **client** being liable for the breach. In serious cases clients may 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 researcher could result in the owner of the data (the client) paying the compensation. Therefore it is essential that researchers ensure that security is adequate to meet their clients' and the Act's needs.

- Researchers 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 researcher must be evidenced in writing.
- Researchers 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?

## Appendix 4

### Protocols for facilitating the sharing of personal data within the public sector

The following list contains sources of information about where there is either legislation, or protocols in place, that facilitate the sharing of data within the public sector.

*These should be viewed as examples rather than as the definitive list.*

The guidance issued by the Department of Constitutional Affairs provides a key overview of the issues.

## Data sharing

### 'Data Protection is an objective of information age government, not an obstacle to it'

(Modernising Government White Paper 1999)

#### Human Rights Act

#### DP legislation

- Disclosure statements/'opt outs'
- Notification

#### Other legislation ('allowed to do'/ultra vires principle):

- Crime & Disorder Act 1998 (Crime & Disorder Partnerships)
- Learning and Skills Act 2000
- Social Security Fraud Act, Proceeds of Crime Act 2002, Registered Sex Offenders
- Children Bill

#### Protocols and other sources of information:

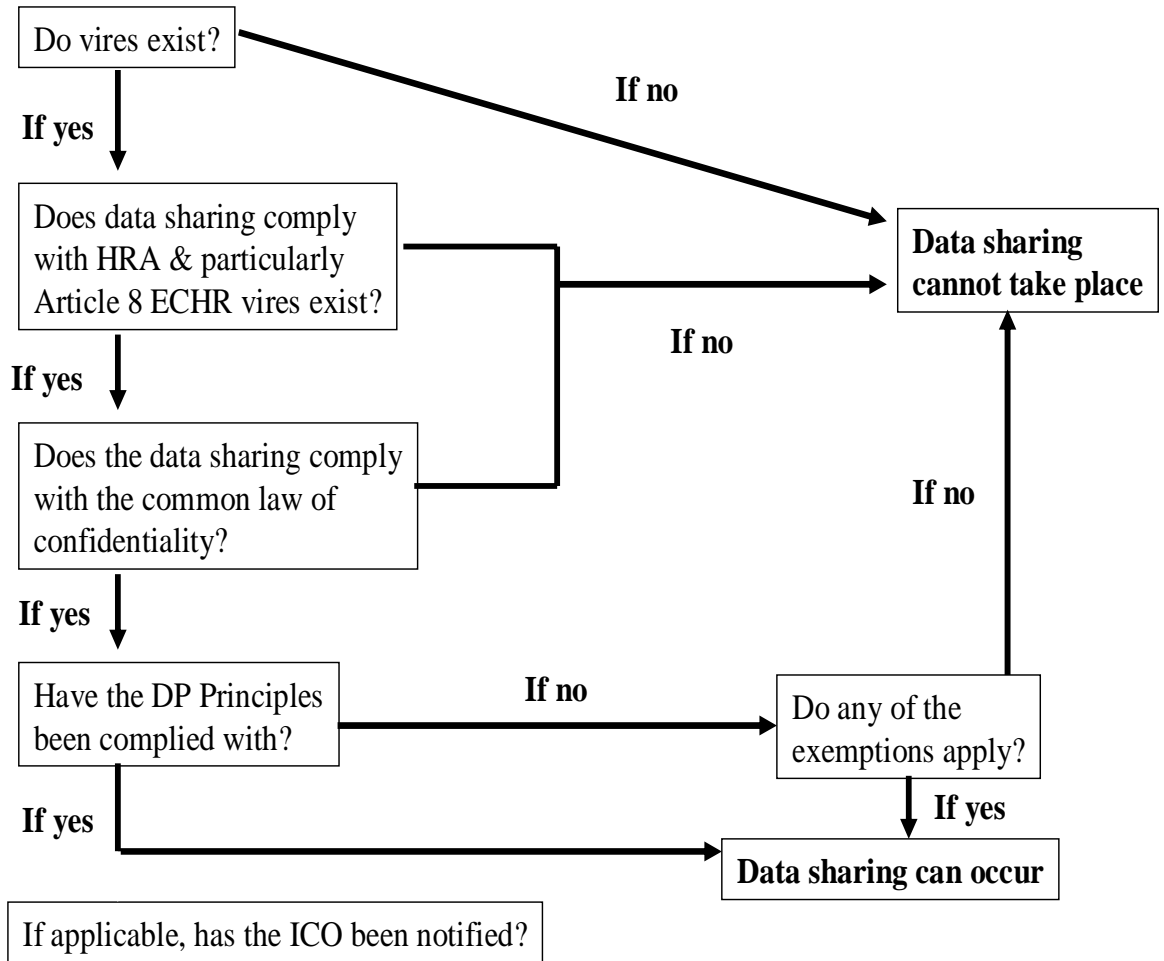
- PIU report: Privacy & Data Sharing
- Information Sharing Toolkit (+ Dept of Constitutional Affairs)
- Caldicot report (health sector)
- 'Information Governance Toolkit' (health)
- Local NHS Trust Ethics Committee
- NHS Care Records Guarantee
- Scottish Executive Health Code of Practice ([www.show.scot.nhs.uk/confidentiality/dataprotection.htm](http://www.show.scot.nhs.uk/confidentiality/dataprotection.htm))
- Information Referral & Tracking (protecting children)
- 'Connexions' partnerships/Sure Start (children & young people)
- ACPO: Crime (inc involving children)
- Partnerships (e.g. local police authority & other agencies & organisations – Staffordshire Multi Agency Joint Protocol for Information Exchange)

### Public Sector Data Sharing Guidance and the law, DCA, Nov 2003

In May 2005, the Department of Health announced that new rules will be launched in 2006 to help patients to keep control over access to their own records including how access will be monitored and policed.

The following diagram provides further guidance to help identify whether or not data within the public sector can be shared without breaking the DPA98:

# Sharing data: lawfully



(Source: Information Commissioner)

## **Appendix 5**

### **COMMON QUERIES AND DATA PROTECTION SCENARIOS**

#### **COMMON QUERIES**

**Q.** Some police forces are willing to provide lists for undertaking research amongst offenders, whilst other ones refuse to do so citing the Data Protection Act 1998 as the reason for refusing (similar situation applies to NHS hospital trusts and lists of patients)

**A.** Releases of this data are governed by relevant protocols – see the lists within Appendix 4.

**Q.** A local authority client is insisting that we keep personal data from research conducted on their behalf for ten years. Is this a requirement under the Data Protection Act 1998?

**A.** There is no requirement within the Act for keeping personal data, beyond the general condition within the 5<sup>th</sup> Principle that the data should not be kept longer than is necessary to fulfil the defined purpose. Once personal identifiers are removed from research data, then the research data is no longer subject to the Act. Therefore it is recommended that this separation is done as soon as is practical. Otherwise, the length of time that personal data is kept is defined by other legislation, the requirements of clients and any internal process requirements.

**Q** Are research projects undertaken by students for their PhD theses at my university covered by the 1998 Act?

**A.** Research undertaken by students are not exempt from the Act. However, the extent to which the university, the student or other parties become data controllers might vary. If the research is conducted to give the clear impression that it is being undertaken by the particular university, then the university is likely to be responsible for ensuring that those undertaking research in their name respect the requirements of the Act. However, if interview samples have been provided by a third party, then as data controllers, the originating organisation needs to ensure that the user meets the requirements of the Act. All students who undertake research that involves the collection of personal data need to be adequately briefed on their responsibilities.

**Q.** Are schools able to provide names and addresses of parents for research purposes?

**A.** The Notification details would identify whether this was a defined purpose. In addition, schools should include this purpose when collecting parents' details updating existing records or creating new ones. A further possibility is for the school to write to parents asking if they would allow their record to be used for research purposes ('opt-in').

**Q.** A research project we've recently undertaken for a local authority identified respondents who were entitled to certain benefits but were not using them. The local authority has now requested details of those concerned so that they can contact them. Should I provide the information they require?

**A.** If the research project was undertaken as a research project then the client cannot use the data for other purposes, such as contacting respondents to make them aware of their entitlements. In order to have done this, respondents would have to have consented for their data to be used for this other specific purpose. In that case, the project could not have been positioned as solely a research project.

**Q.** We are conducting a crime survey with victims of crime on behalf of a Police force. Currently the survey includes a re-contact question which asks whether individuals would be willing to be re-contacted for future research. If respondents unfortunately become the victim of a second crime and appear again in the sample supplied by the police can we still contact them, even if they refused the re-contact question?

**A.** The wording of the current re-contact question is key to this issue. If a client wishes to include repeat victims, the wording of the re-contact question must specifically state that the follow-up would only be in relation to the first specific crime. Thus if they were to reappear in the sample frame due to becoming a victim for a second time, the researcher would not have to screen out those who refused the initial re-contact question.

**Q.** We are conducting a telephone survey on behalf of some academic clients who in turn have a government client. The academic clients are wanting to analyse our survey data in the context of some government data and then look at it again in 10 years time. The individuals would be identifiable as there would be an identifier kept on the fused data. Is it okay to fuse the data in this way?

**A.** Yes, although the respondents must have consented to being identified, the purpose and the length of time the data is to be retained.

**Q.** What is the Freedom of Information Act?

**A.** The Freedom of Information Act creates a right of access to official information and places a duty on public authorities to publish information. ([www.informationcommissioner.gov.uk](http://www.informationcommissioner.gov.uk))

**Q.** What is the difference between Freedom of Information and Data Protection?

**A.** The Data Protection Act enables individuals to gain access about them; the Freedom of Information Act enables individuals to gain access to all information held by public authorities. It should be noted that personal data is an absolute exemption under the Freedom of Information Act and as such this legislation can not be used to gather personal data about other individuals.

## **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 researcher 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 researcher 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 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 providing they are then used for 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 research dataset. Overall, there will be joint data controller responsibilities for this project between client and researcher;
- Whether West Barsetshire has Notified 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** 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 researcher can indicate that there appear to be these other types of errors, but not the individual cases concerned;
- Complaints can be fed back– 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 research project and that any information provided to the client at a personalized level will only be used for 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.

## **2. Social and Opinion Research**

### **2.1 Scenario**

Social and Opinion Surveys (SOS) have received a brief from a new client, the University of Barseghire, for a quantitative fieldwork only project to be conducted amongst a sample of students currently studying at the university about the provision and usage of recreation, leisure and medical facilities within the area. The university states that they could provide a list of names and addresses for sampling purposes if this would be helpful. The proposal specifically states, firstly, that the identity of the client must not be disclosed to respondents, secondly, that the researcher will be expected to provide the findings to the client in an attributable form, thirdly, that depending on the findings they may wish to conduct follow-up interviews with some of the respondents. The client claims that under the 1998 Act the researcher will be acting within the law, and that under the Act permission from respondents to do any of this is not required as it is a survey research project.

### **2.2 Analysis**

- If the university provides the sample then whilst they would remain data controller of the original file. However, if SOS then develop a version of this to manage the project then it is likely that the researcher and the university will have joint data controller responsibilities. If the researcher is responsible for sampling (i.e. finding respondents) then they are likely to be the data controller for that file, especially if the project is conducted in the name of the researcher as a research project.
- If the university provides the sample, then respondents must be told this by interviewers if they ask about the source of their name and address – at some point in the interview.
- The university must have notified research as a purpose for processing any data used as a sampling frame.
- Research agencies may in some cases simply act as data processors on behalf of a client. However, in a case such as that described attributable data can only be provided to the client if the research is conducted in the name of the client; it is made clear to respondents that their personal data will be provided to the client, and, the respondent has consented to this disclosure. In addition the purpose(s) for which the data will be used must also be made clear and respondents must be given the opportunity to opt-out of their data being used for any purpose(s) to which they object. The client must ensure that these expectations are met and that the data is not used for any other purpose. If the client wants to use the data for direct marketing purposes, then the direct marketing provisions in the Act must be met.
- If SOS undertake the sample selection themselves and conduct the interviews in the researcher name then the identity of the client does not need to be disclosed.
- Re-interviewing can only be undertaken if permission has been gained at the initial interview.
- It appears that Sensitive data (i.e. medical information) might be collected in the survey. However, whilst explicit consent is not required if the information is being used solely for research purposes, it would be good practice to mention in the pre-ample to the interview that some questions will cover medical issues and reassure respondents that this will be kept confidential.