# MRS/SRA

# Data Protection Act 1998: Guidelines for social research

## April 2013


**CONTENTS**

## FOREWORD

*Consumers and citizens are becoming more and more aware of the value of their personal information, its value to them in terms of what could happen if it gets into the wrong hands or is misused in some way, and its commercial and financial value to the organisations who collect it. So it's more important than ever that organisations collecting and processing personal information take privacy and data protection seriously. Clear and relevant guidance written by representative bodies with expert knowledge of a particular sector is invaluable to organisations looking to comply with the law. It is also a clear signal to consumers that their rights and concerns are important to the sector. I welcome the focussed and practical advice contained in the guidelines produced by the Market Research Society and the Social Research Association and I'd advise all concerned to follow it closely. Consumers and citizens are wising up and will start picking and choosing between brands that respect their privacy and those that do not. Don't get left behind. It's not just the Information Commissioner you'll have to deal with.*

**Christopher Graham**
**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 SRA members 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 five 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.*

**Patten Smith**
**SRA Chair**

**Debrah Harding**
**MRS Chief Operating Officer**

## 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.

In 2009, 32% of all queries received by the MRS Codeline service related to data protection issues. Whilst this represents a fall from the 60% at the time the guidelines were first published in 2005, this updated version contains new areas of guidance following recent discussions with the UK Information Commissioners Office (ICO), the UK regulator responsible for the Data Protection Act 1998, on the use of incentives in research projects. Data privacy remains a very dynamic field of legislation and regulation. A review began in May 2009 of the current EU Data Protection Directive, to which the market research sector in Europe has already contributed a response. Following a spate of high profile breaches of the UK law, the ICO has been granted increased powers covering the notification of data breaches, a new fines structure for deliberate offences and Part 8 of the UK Coroners and Justice Bill provides new powers to conduct data privacy audits. In May 2011, the ICO launched a new code of practice covering data sharing, and changes to the rules on cookies and similar technologies for storing information. There is also a new EU ePrivacy Directive close to enactment, tougher rules are likely for behavioural targeting using social networks data, and greater protection for children using the internet. All this underlines the fact that data privacy remains a very important influence on the everyday activities of researchers. In addition the European wide RESPECT code of practice for social researchers includes a section referring to data protection issues.

However, the Data Protection Act has benefits for research:

- legal commentators see the UK version of the Directive as providing a balance between preventing the exploitation of personal data whilst respecting the value of such data within the modern world. Despite recent breaches of the Act, the UK also have a regulatory framework that still welcomes discussion first rather than seeking confrontation when issues emerge;

- research, as defined within the latest version of the MRS Code of Conduct (April 2010) and SRA Ethical Guidelines, 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 research , as direct marketing, but as reflected in the MRS Code of Conduct, and the following guidelines, defining the boundary between ‘commercial’ activities such as

marketing, whether in the private or public sector, and research remains a key issue;

- it gives more weight to the professional codes, in particular those key clauses that are designed to protect the rights of respondents - first codified by the research sector world-wide well over fifty years ago;

- because of the legal implications, it focuses the research sector 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, continue to be aware of the implications for the research sector.

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 process guidelines referred to below*).**

The following guideline is based on the detailed advice for MRS members and MRS Company Partners contained within ***'Market Research & the Data Protection Act 1998: Advice for Members',*** and also complements two further guidelines on how the 1998 Act impacts upon research processes: ***'Market Research Processes and the Data Protection Act (DPA) 1998',*** produced by the MRS, 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. **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;
- Personal data already in the public domain doesn't normally require consent to be sought to be used, but this is not always the case (e.g. when publicly available data is enhanced with information from other sources).
- 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. However, it should be noted that removing personal identifiers requires more than removing names and addresses, other apparently generic information (demographic or geographic for example) can identify an individual;
- 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' opt in/out requests 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 they 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 other 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);
- Permission to re-interview must be obtained at the time of the first interview, except when re-contacting for quality standards purposes (e.g. ISO 20252);

- Personal data collected in the name of a researcher can only be transferred to a client, even if for research purposes, with the explicit consent of the individual respondent;

- Ensure that any sharing of personal data, for example, used for sampling purposes or collected in a survey meets the ICO code of practice for Data Sharing (see Appendix 4 of these guidelines);

- If they ask, respondents have the right to know the source of any personal data used (if there is a source) to recruit them;

- Interviewers must return or destroy any sample containing personal details sent to them and such information cannot be used for any other purpose e.g. to create their own recruitment lists;

- When recruiting for qualitative research, respondents must be informed about any recording or observation at the time of recruitment and at the beginning of the qualitative research;

- The data controller responsibilities must be clearly identified and delineated between the parties involved in any research e.g. client, researchers, sub-contractors, etc.

- Where a client-supplied sample is provided, or sample is provided by another other third party, check on the ICO web site that the client and/or third party has appropriately notified the purpose(s) and disclosures for their personal data e.g. that the notification includes research as one of the purposes;

- Researchers and research suppliers have been notified and that the notification is adequate. Your organisation may have appointed someone to look after data privacy issues who can help;

- All parties to a research project must be bound by a written contract this includes clients, researchers and sub-contractors;

- Client-branded incentives cannot be used when undertaking research projects as this would be a form of promotional activity which is beyond the research purpose;

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 third party other than those identified at the time of data collection without have gained the respondent's consent during the initial research/data collection;
- using respondent 'verbatims' from a research project in a report which might be easily attributed by a reader to a particular respondent without having gained their prior permission;
- providing "anonymous" data to a client at such a level where identification might be possible e.g. full postcode level.

**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.

**Interview**

An interview is any form of contact intended to obtain information from or about a respondent or group of respondents. This can involve passive as well as direct contact.

**Research**

Research is the collection and analysis of data from a sample or census 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 interviews and group discussions, observational, ethnographic and panel studies.

The MRS Code of Conduct contains other definitions of potential interest to readers of this guideline.

## SECTION A: PRINCIPLES OF THE DATA PROTECTION ACT 1998

All processing of personal data must conform to the requirements of the UK Data Protection Act 1998 (for more information see http://www.legislation.gov.uk/ukpga/1998/29/contents)

Appendix 1 summarises the key Principles within the 1998 Act.

***The key concepts underlying the Act are:***

- **Transparency** – ensuring individuals have a very clear and unambiguous understanding of the purpose(s) for collecting data and how they 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[1].[2]

When collecting research data the purpose of the data collection must be transparent. All assurances made to respondents must be honoured. If data are 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, and respondents must be given the opportunity to opt out of any purposes that they find unacceptable.

If respondent's details are to be *kept* on a client or researcher held database for further research, respondents must be made aware of this at the initial interview and given the opportunity not to be re-contacted. However, this excludes follow-up interviews conducted solely for quality control purposes e.g. 'back-checking' requirements as detailed in ISO 20252.

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 sector has developed a detailed description of permitted disclosures and associated conditions applicable to research projects. These categories are summarised within Appendix 2.

### Key definitions

[1] This does not apply to any re-analysis of the anonymous data as long as individuals cannot be recognised.
[2] For covert observation see clause 7.5 of the Socio-Legal Studies Association guide to ethical practices http://www.slsa.ac.uk/images/slsadownloads/ethicalstatement/slsa%20ethics%20statement%20_final_%5B1%5D.pdf

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, etc. 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 MRS Code of Conduct no longer includes any recommended period to keep primary data records – this is for researchers to decide based on the type of research, other legal requirements and contracts with clients or internal administration needs.

At the planning stage researchers must discuss with clients whether identifiable data are to be shared with them. Identifiable data can be collected and passed to a client during a research exercise on the condition that they are used only for the purpose for which they were 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 participate in research 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 the personal data *must* be disclosed if a respondent requests this information. However, this information can be disclosed at any appropriate point during the research, rather than when the respondent requests it e.g. at the end of a research interview rather than the beginning if the respondent consents to participate on this basis.

If conducting a research project which involves collecting 'sensitive personal data' (as defined in the 1998 Act – see the definition of 'Sensitive data'), any introductory

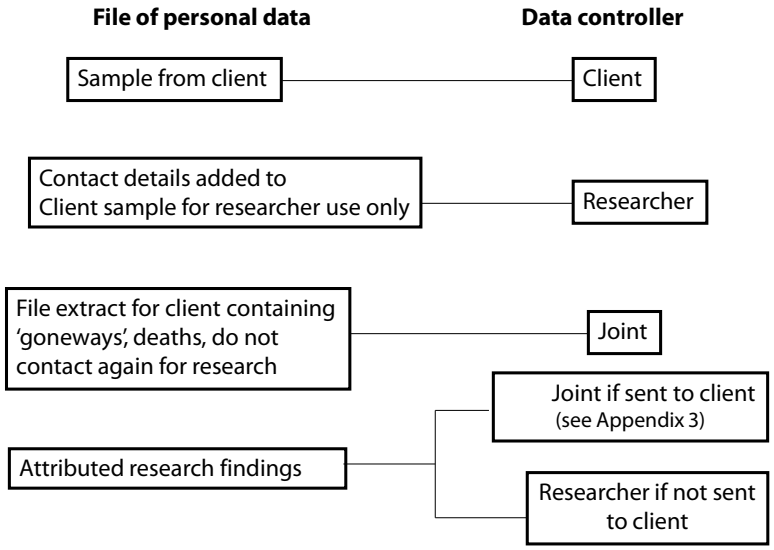
text, such as the preamble of a questionnaire, should include sufficient information to ensure that respondents are aware such information is to be requested. For example to describe a research project as covering "leisure activities" and to collect data about usage of the local swimming pool would be considered sufficient description to collect such data. However it would not be sufficient when collecting data about respondent's sexual activities – if this type of information were to be collected as part of a research project, respondents must be aware of this from the beginning of the process.

The Act requires data collectors to obtain prior consent to collect data defined as 'sensitive'. This condition has been met when a person agrees to take part in the project (see Appendix 1).

**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 ICO (unless exempt) Figure 1 describes the data controller responsibilities between clients and researchers:

**Figure 1: Defining data controller responsibilities in the Research Process**



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.

See Appendix 3 for more information.

**Data Processors**

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

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 Figure 1. Data processors are sometimes located outside the EEA and there are model clauses that could be used in such situations (see Section 1.7 below for more details). There is also the need for statutory written contracts in certain situations, for example, with data processors.

**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 legally 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;
- Data about an employee's job will not usually constitute personal data. For example, asking a procurement manager to describe the procurement policy of the organisation would not be personal data. However, asking a named procurement manager their attitudes towards the procurement policy would constitute personal data.

**Personal 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. a fifty year old widow with a medical exemption certificate). Identification could be through a person's voice, or even their views (e.g. in some cases a verbatim used from a qualitative group) could identify someone particularly if the research universe is small as in the case for b2b and employee research

'Personal data' under the 1998 Act are data that identify an individual, or would enable them to be identified, where the processing is wholly, or partly, using automated means (also see Manually held Data,) or where it is non-automated processing of personal data which forms part of a 'filing system' or is intended to form part of a filing system. This can cover information whether in a person's personal or family life, business or professional capacity[2].

[2] See: http://www.ico.gov.uk/news/current_topics/what_is_personal_data.aspx for guidance on what constitutes personal data.

The Act does not include non-recorded data, such as listening in to telephone interviews as they are being conducted – this is covered by other regulations, but the Act would apply if the live interviews were electronically captured.

Data that is covered by the Act includes electronic, manual and recorded data - anything that captures information which is sufficient to 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, where their role and/or job function is not unique (e.g. Account Managers etc) and that simply describes an individual's role within an organisation, or where the data is related to a general role rather than an individual, is not classified as personal data. So, if a research project of IT directors was collecting data about the responsibilities of IT directors and the research 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 respondents, and a full demographic profile of each individual, then the data would be personal data.

**Manually held Data**

The UK Court of Appeal has ruled that only personal data held in manual files which is held in a 'relevant filing system' and 'only if they are of sufficient sophistication to provide the same or similar ready accessibility as a computerised filing system' are covered by the Act. 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.

The ICO website includes guidance on determining what data are covered by the Act: 'Data Protection Technical Guidance Determining what is Personal Data', including illustrative examples.

**Notification**

'Notification' is the annual reporting process informing the ICO 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. A new fee structure for Notification based on number of employees was introduced on October 1st 2009.

It is a statutory requirement that all data controllers need to ensure that all relevant activities involved in processing personal data are notified to the ICO using the forms (Part 1 and 2) available either on their web site (www.ico.org.uk) or via the ICO helpline. Data controllers must notify annually. All notifications are in the public domain (see www. ico.org.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. a citizen panel).

The ICO has ruled that where research might be a logical purpose related to the main activities of the organisation, it doesn't necessarily need to be specifically mentioned. An example would be undertaking customer/citizen satisfaction research where services, or service centres, are a core activity.

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

**Sensitive data**

This is defined in the 1998 Act (section B clause VII) 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.

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. (See Section A: Consent), Generally in terms of research interviews, as long as the key rules of transparency and consent, are followed and are 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 (FOI)**

The FOI creates a right of access to official information and places a duty on public authorities to publish information. The Act became law on the 1st January 2005. However, whilst the Information Commissioner is the regulator for the Data Protection Act within England, Wales and Scotland, the ICO's powers covering the FOI Act only apply to England and Wales, there being a Scottish Information Commissioner responsible for the FOI within Scotland. The difference between the Freedom of Information Act (FOI) and Data Protection (DPA) is that the DPA enables individuals to gain information about themselves whereas the FOI enables individuals to gain information about public authorities. Research data and research projects are not exempt from the FOI, but personal level data is usually exempt from third party requests, and as such generally 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. The FOI exemption covers all types of manual data. However, personal data might be released under a FOI request where it relates to an individual's public responsibilities. 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, requires 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 under FOI 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 projects are managed, progress reports and reports on contract management
- Questionnaires
- Reports based on research findings
- 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[3]. This can be provided in a summarised form.

FOI requests can at present only be made to public bodies, but requests to third party organisations working for public bodies is under consideration.

Data would not normally be exempt simply because they are of poor quality, from flawed methodologies or not considered 'fit for purpose'.

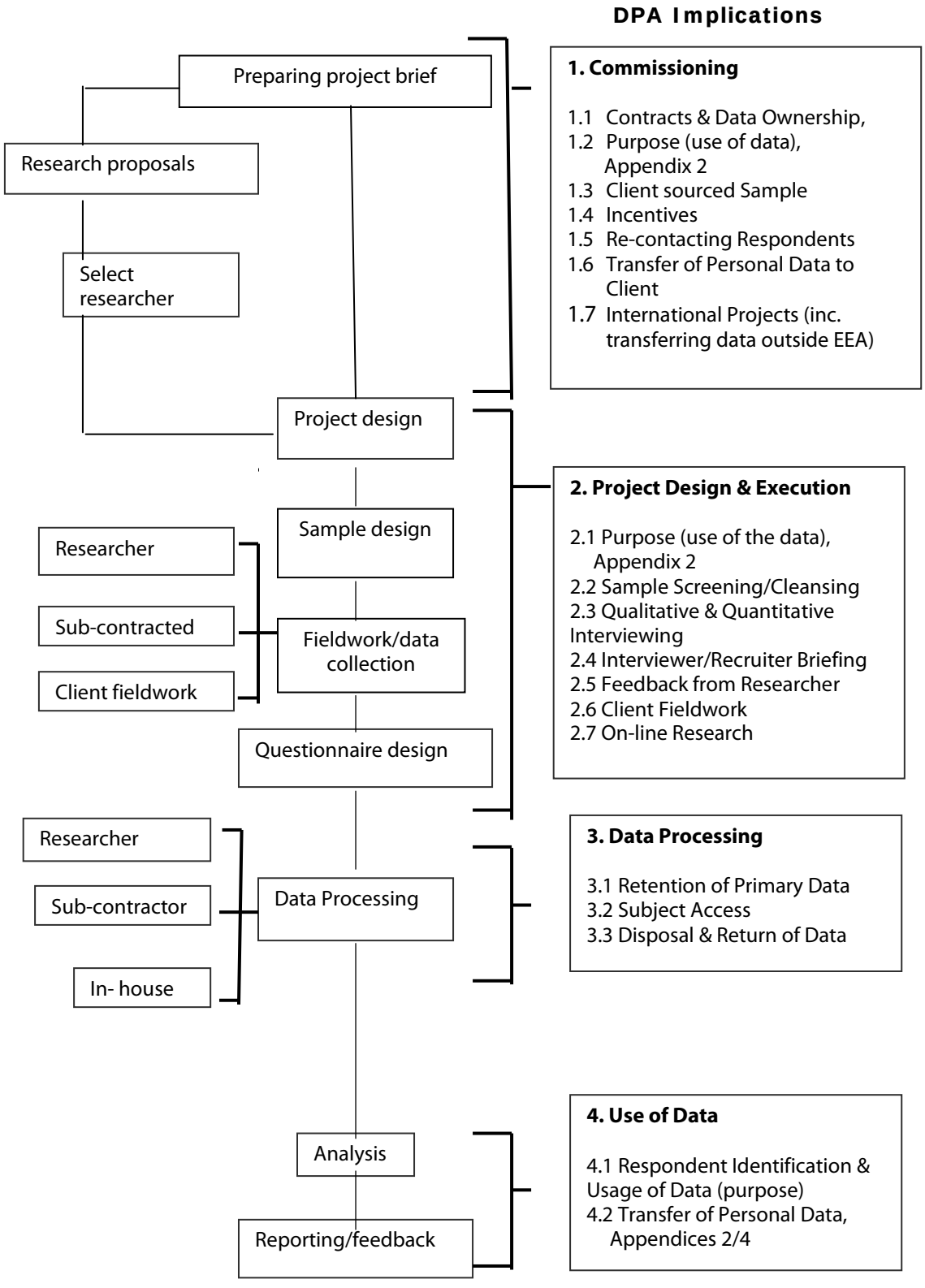
Further information on the FOI for England and Wales is included on the Information Commissioner's web site, and for Scotland see www.itspublicknowledge.info .and www.scotland.gov.uk/socialresearch (the Chief Researcher in the Office of the Permanent Secretary, Analytical Services Group within the Scottish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

[3] The courts have given a broader interpretation to the meaning of data "held" by a public authority (e.g. in the Common Services Authority decision in the House of Lords stating that barnardizing data already held might be necessary to satisfy a request even though baranardized data was not strictly speaking held by the authority).

## 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.

**Figure 2: 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 clients are supplying data for sampling or supplying it 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 researchers (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 clients supply data for sampling purposes the following conditions apply:

- Clients must have completed their annual notification with the ICO– this can also be checked on www.dpr.gov.uk.
- Notifications must ensure that data is used for “research” purposes. Notification details can be checked via the Notification Register on the ICO website
- If a project includes data collection for purposes other than purely for research the client must ensure that their Notification includes this additional purpose(s).
- Clients should check that researchers are aware of their responsibilities (and those of any sub-contractors) under the DPA98.
- Clients should ensure that contract/terms and conditions contain clauses that adequately cover the data protection responsibilities of researchers and any subcontractors, such as the need to ensure that any personal data provided by clients (e.g. NHS hospital trust patients records used for sampling) will be

securely transferred and held; not used for any purpose other than as specified in undertaking the specific project; securely destroyed or returned to clients once projects have been completed.

- Clients need to consider whether or not researchers/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 a client plus research findings. Shared ownership of the data would need to be 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 data subjects. This is not applicable in instances where a client passes a sample frame to a researcher on condition that the data are being passed for the completion of a contracted research project only. At the planning stage consideration should be given if research data at a personal level are to be shared with more than one client and the appropriate explicit permissions incorporated within the research design 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. As mentioned earlier, the ICO has now issued a code of practice covering data sharing. See Appendix 4 for further details on data sharing and Appendix 3 for Data Security issues.

### 1.2 Purpose (use of personal data)

Clients should clearly state within briefs if researchers are required to provide personal data collected within a 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 DPA98 that occurs while personal data are 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 DPA98 by a researcher would result in the owner of the data (the client) paying the compensation. It is essential that clients check that researchers have adequate security processes to meet clients' and

the Act's needs and that contractors have understood and accepted their responsibilities. A data controller cannot 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 at a personal data level then this should be specified to respondents and permission obtained prior to the information being released (see Appendix 2 for disclosure rules).

- Care should be taken if known ex-directory or Telephone Preference Service (TPS) numbers are to be included in a telephone research project. Interviewers should be briefed on how to respond to any queries/complaints from contacts. Any marker on the file stating that the individual does not wish to be contacted for social, market or research purposes must be respected (also see Appendix 2).

- If personal data from a research project are to be used for any purpose *other than research* then samples may need to be pre-screened to remove any people who have stated they do not wish to be contacted in specific circumstances. See Section 2.2, below for full details.

- In instances where clients have supplied their own database for sampling respondents have 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 clients to researchers must be evidenced in writing.

- Researchers need to agree with clients how to respond if 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.

- 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, unless a data sharing agreement is in place which has been approved by the appropriate government departments. If some data merging is to take place during the research analysis stage, it is preferable that this is undertaken by the researcher.

### 1.4 Incentives

An incentive is any benefit offered to respondents to encourage participation in a research project.

The ICO has recently ruled that client goods or services, or vouchers to purchase client goods or services, should not be used as incentives in a research project as this would promote the client's products or services, which is outside the scope of 'research' as a purpose. This means that if clients insist on providing their own incentives, such projects cannot be described to respondents as being research. Such projects **must** conform to the rules in the *MRS Regulations for Using Research Techniques for Non-Research Purposes*. The exercise **must not** leave respondents with the impression that they are taking part in a research project and the additional purpose must be made clear.

*An example: A local authority wishes to conduct a survey amongst local residents about their attitudes towards the services it provides. In their tender for the project they state that all respondents will be given a voucher giving them a free two hour session at any of the leisure centres they own. If the client insists on providing this as the incentive, the project cannot be described as a confidential research project and must conform to the rules laid out in the* MRS Regulations for Using Research Techniques for Non-Research Purposes.

The same rule applies to a client sourced/branded 'thank-you' as if the respondent has already participated in the interview, this 'thank-you' has no purpose directly related to the research.

For more details see the new *MRS Guidelines for Using Incentives*.

### 1.5 Re-contacting Respondents

The Data Protection Act 1998 specifies a number of conditions that must be met before processing is considered "fair" (the first data protection principle). One of the requirements is that respondents are aware of the likely consequences of participating in a data collection exercise. If a respondent's details are, or likely, to be used for a further research (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. The wording of any re-contact question needs to be agreed with clients at the planning stage to cover any planned or possible consequential interviews.

When contacting potential respondents, 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.

### 1.6 Transfer of Personal Data to Client

At the planning stage Clients need to decide whether research projects will be conducted in the name of a third party (e.g. 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 they are used only for the purpose for which they were collected (e.g. research purposes), and, if the data are 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.

### 1.7 International Projects and transferring data outside the EEA

The following conditions should be considered if any identifiable data is to be sent outside of the European Economic Area (EEA - the countries subject to the Directive on data privacy):

- the country has been approved by the European Commission as having adequate levels of data privacy legislation. The ICO website contains under Data Protection Act, International Transfers, a link to the europa website and the list of currently approved countries[4].

- contract with the receiver that they have adequate data security to meet the requirements of the Data Protection Act 1998. There are model clauses agreed at EU level for this. They fall into two categories: data being transferred to a data

[4]Transfers can also take place if there is in all the circumstances "adequate protection" i.e. self-certification. For example, such self-certification might be applicable with the processing of very innocuous personal data even for research purposes.

processor; data being transferred for use by a third party. For details see: **www.europa.eu.int/comm/internal/en/dataprot/news/index.htm**

- consent of data subjects;
- in the case of data being transferred to the U.S.A., it may be possible to use the "Safe Harbor" agreement (this applies to USA companies only – see 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 are stored or transferred using online or digital methods.
- Clients should:
  - agree with the researcher if data are to be transferred;
  - define where data are to be transferred;
  - agree appropriate permissions, if necessary, in the questionnaire to allow data transfer to take place and/or include in contracts with data recipients standard data transfer clauses mentioned above.

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. 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.

- **Within the EU**

Although the 1996 EU Directive contains standard principles covering all EU countries and the national laws in each country are deemed to provide an adequate, and common, level of protection, there are differences across the EU that can impact on research projects being conducted in EU countries outside the UK – Germany being a prime example. For more details see the annual reports from the EU Article 29 Group at: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/annual_reports_en.htm

## 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 respondents).

For projects conducted for a purpose in addition to research, any data collection materials (e.g. questionnaires) 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 (e.g. by providing an 'opt-out').

### 2.2 Sample Screening/Cleansing

In instances where clients supply researchers 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) may require 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 Section 1.3, above 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 by telephone or fax 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 Telephone or Fax Preference Services (depending on the data collection method).

### 2.3 Qualitative & Quantitative Interviewing

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

- It must be made clear who a 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 'MRS *Regulations for Using Research Techniques for Non-Research Purposes* (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 recorded observation studies, where no specific invitation to attend has been given, the researcher should follow the CCTV Code of Practice (or its fundamental principles if not using CCTV equipment) produced by the ICO (for full details of the code see **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. Clients need to ensure that contracts with researchers or other data processors cover 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 legally responsible 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. Other points to consider include:

- 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 future sample selection 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 by the client.

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/ guideline, 'Market Research Processes and the Data Protection Act (DPA) 1998'. In particular, it is important that those who conduct 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 Section 1.3, 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 are found?

- If telephone research – does the list contain ex-directory numbers?

- Security of the data – are procedures in place to ensure the data are transferred and held securely whilst off-site?

- Return of the data – are procedures in place to ensure the secure 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 researcher undertakes online research, then the web site must contain sufficient information regarding their data privacy policy. The same applies if a client undertakes their own online research projects. The Information Commissioner has produced a set of general guidelines for company web sites and the MRS and ESOMAR have developed guidelines covering online market and social research (see respective websites for details). The new ICO rules on cookies mentioned in the Introduction to these guidelines, introduced on May 26th, 2011, brings the UK's rules into line with European law. The main change is that cookies can only be placed on machines where the user or subscriber has given their consent. This requires users of that equipment to be provided with 'clear and comprehensive information about the storage of, and access to, that information, and has given his or her consent' (see http://www.allaboutcookies.org/ and http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/cookie_rules_prepare.aspx).

## 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 are held at an archive storage facility, either off- or on-line, the security measures must be appropriate and adequate to meet the security needs of the client data stored.

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

- Clients and researchers 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 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, and contracts with clients or internal administration needs.

### 3.2 Subject Access

When clients or researchers hold respondent information in an identifiable format (e.g. client-supplied lists held by a researcher used as sampling frames, completed questionnaires etc.) respondents have the right to see the personal data held about them. This includes any data held in electronic format, certain forms of manual data such as questionnaires and any digital/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 to a researcher covers information provided by a client who is the data controller, then only the client can deal with the request (e.g. the sample file provided by the client). When data are held in an unidentifiable format the data fall 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). Other points to consider include:

- 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 may still have to provide access under the Act to satisfy the request.

- For a subject access request, personal data do 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 meeting a subject access request, personal data obtained during research covering other individuals must not be disclosed (e.g. other participants in a group discussion).

- 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 to be charged by data controllers for subject access requests (the fee can vary for health and educational records). 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 (including manual and digital/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)

Contracts with researchers (and with any data processors) should clearly specify whether any personal data supplied by clients should be destroyed or returned to the client.

For quality standard purposes it is only necessary for researchers to keep primary data which are 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 researchers until either these are returned, securely, to clients or destroyed by researchers. Particular care should be taken if data are stored online.

- Clients should check that researcher's have similar procedures in place for any data held by sub-contractors involved in a project (e.g. interviewers and recruiters; data processors responsible for coding/analysing personal level data).

- Clients should ensure that the destruction of data is adequate for the confidentiality of the data being destroyed (see requirements within ISO27001).

- 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)

Data collection preambles, documentation, etc must be sufficiently clear to ensure there is no ambiguity when gaining permission from respondents.

- The identity of respondents and/or attributable comments can only be released with the express permission of respondents.
- Clients must not use 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 releasing identifiable research results (e.g. during a hospital out-patient's satisfaction interview a respondent criticises the performance of a particular member of staff without any consent being sought from the patient to enable details to be used other than in anonymised research. The comments are fed back to the individual member of staff who then confronts the patient when they next visit the hospital).
- Care must be taken if data from a research project are 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 respondents and this must be collected at the time of the initial data collection.

- If the data are 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 1.7 above 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

- Releasing audio, digital and video recordings or transcripts to clients:

  - All individuals concerned must have consented to the release of data to third party and the purpose(s) to which the data will be put by the third party.

  - If an individual withdraws consent after a group or interview takes place, the researcher must not pass the data to the client.

  - When primary data are released they must be labelled with the details about the purposes for which they can be used.

  - Recipients of personal data must not use them for any purpose other than that for which consent was gained when collected.

  These conditions should be stated in the contract between clients and researchers.

**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[5] of the Act is met, and

    - in the case of sensitive personal data , at least one of the conditions in Schedule 3[6] 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

---

[5] 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.

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

level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

**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, researchers 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 goneaways.*

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 client database in order to prevent over researching individuals.

*An example: A university supplied a list of recent graduates to a researcher to conduct a student satisfaction project by 'phone. 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 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. If the survey is conducted online, a special e mail link, or freephone telephone number may need to be provided to enable a respondent to contact the client

*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 (including a 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 are 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) this would include recordings from group discussions, where it might be necessary to hide the identity of any participants who had not consented to their personal level data being passed back to the client.

*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 rules in the *MRS Regulations for Using Research Techniques for Non-Research Purposes*. 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 recordings 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 are 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 adequate measures are in place to ensure the security of personal data. This applies to all organisations that hold personal data as part of a research project. 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 the transfer of personal data; storage; and use in 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.
- Ensure unnecessary data is not provided to third parties simply because it is easier to do this than undertake any pre-processing.
- Clients and researchers should consider the following checklist regarding security when assessing whether their own technical and organisation measures, and those of third parties, are appropriate**:**
    - Are the electronic systems protected by a level of security appropriate to the data held?
    - Where personal data are stored online, are there appropriate security measures in place to prevent unauthorised access?
    - Is there a data privacy policy covering portable media and hardware; is this adequately enforced and audited?

- Are technical measures and policies in place to restrict access, including remote access, to systems holding personal data (e.g. passwords, PIN numbers, firewalls)?
- Are technical measures (e.g. encryption) in place to secure data during transit (e.g. to subcontractors and interviewers)?
- How is the data stored/transferred by sub-contractors and interviewers? Is it adequate and appropriate?
- Are the premises on which the data are held secure?
- Is access to the premises restricted?
- If the data are held in manual systems e.g. paper files, discs, memory sticks, CDs, microfilm, and microfiche, is access still restricted or secure? Has consideration been given to using more secure forms of storage?
- Are copies of printouts, obsolete back-up tapes, CDs, etc disposed of 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 new and existing staff (including contractors) trained and made aware of their responsibilities to safeguard the personal data?
- Are data privacy policies and processes regularly updated and audited?
- Do risk assessments include data privacy issues (data privacy by design)?
- Has the ICO 'Promise' been adopted, or considered?
- Are there quality standards in place (e.g. ISO 27001)?
- What is the electronic archiving policy? Are identifiable research data permanently archived? Is so are the archiving procedures sufficiently robust?

## Appendix 4

### Data Sharing

The guidance issued by the Department of Constitutional Affairs provides a key overview of the issues: 'Public Sector data sharing: guidance on the law' (www.justice.gov.uk).

In addition, the Ministry of Justice commissioned a review of data sharing, published in July 2008. The report, 'Data Sharing Review' by Richard Thomas and Mark Walport, plus responses, is also available on www.justice.gov.uk

In May 2011, the Information Commission issue a code of practice covering Data Sharing. The main points are summarising later on in this appendix, and full details can be found on the ICO website: www.ico.gov.uk/for_organisations/data_protection/topic_guides/data_sharing.aspx

### 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.

### Human Rights Act

### DP legislation

- Disclosure statements/'opt outs'
- Notification

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

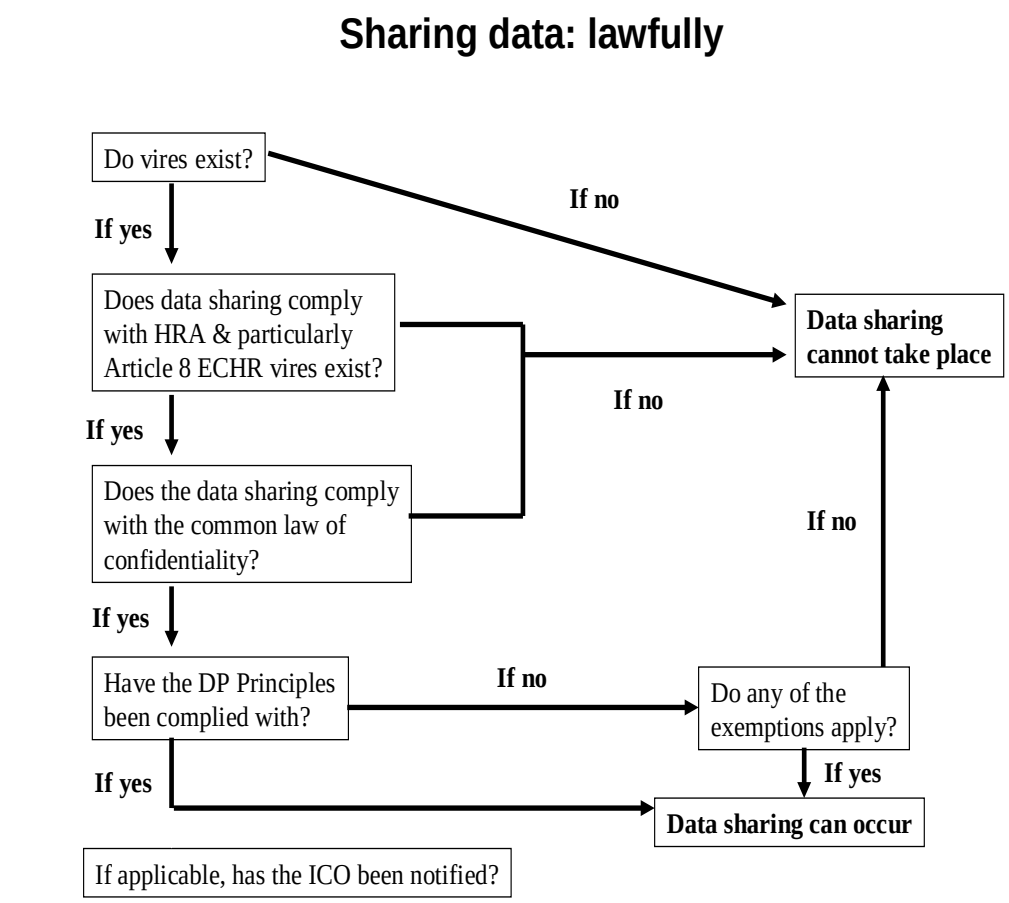
- Crime & Disorder Act 1998 (Crime & Disorder Partnerships
- Learning and Skills Act 2000
- Social Security Fraud Act, Proceeds of Crime Act 2002, Registered Sex Offenders
- Children Bill

### Protocols etc

- 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)
- 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)

Figure 3 provides further guidance to help identify whether or not data within the public sector can be shared without breaking the DPA98:

**Figure 3: Sharing data lawfully**




**(Source: Information Commissioner)**

### ICO Data Sharing code of practice: key points

As the Information Commissioner states in the forward to the new data sharing code, whilst the term used in the Data Protection Act is 'data sharing', it's really about the different types of disclosure of personal level data, in an increasingly complex world. The code also includes data sharing checklists containing a step by step guide to help users decide whether or not personal data should be shared.

The code covers the main categories of data sharing:

- **Systematic – routine sharing for an agreed purpose**. For example, a research agency may share personal level data from a panel with specific clients, for research purposes only and with the consent of panel participants
- **Ad hoc or 'one-off' data sharing**. This might occur when an agency wishes to provide feedback to the client on possible errors in a sampling frame.

- **Sharing with a data processor**. This reminds data controllers to ensure that they have an appropriate written contract with data processors. For example, providing an agency with personal level data in order to conduct interviews

- **Sharing within organisations**. Different departments or divisions etc within an organisation may have differing approaches to data protection. This needs to be considered if, for example, personal data from a survey is provided to more than one department within the client organisation.

The ICO reminds users that different legal requirement apply in the public and private sectors (see the general introduction in this Appendix).

The main factors to consider when deciding to share personal data are described in Section 5. Points you need to consider are:

- What is the sharing meant to achieve?
- What information needs to be shared?
- Who requires access to the shared personal data?
- When should it be shared?
- How should it be shared?
- How can we check the sharing is achieving its objectives?
- What risk does the data sharing pose?
- Could the objective be achieved without sharing the data or by anonymising it?
- Do I need to update my notification?
- Will any of the data be transferred outside of the European Economic Area (EEA)?

In Section 6, the code reminds users that data sharing may need to be mentioned in any privacy notice – why the data will be shared, and who it will be shared with (e.g. the survey client). Particular care is necessary in cases where the data is sensitive; sharing is likely to be unexpected or objectionable; is likely to have a significant effect on the individual; sharing is widespread, or for a range of purposes.

The code also provides advice covering data sharing following a merger or takeover – but this could apply in situations where public services are outsourced to a third party.

Data security is covered in Section 7 (underlining the advice given in Appendix 3 of these guidelines) and best practice Governance is covered in Section 8, including content for data sharing agreements.

In Section 10, covering things to avoid, the code specifically refers to cases where anonymised statistical information might be sufficient for the intended purpose, as often might be the case in research projects.

Section 13 reminds public sector organisations that Freedom of Information legislation can apply to data sharing arrangements, and this could cover data shared by a private sector organisation with a public sector body.

Section 15 contains the checklists covering the following key issues:

- Is the sharing justified?
- Do you have the power to share?
- What to consider if you decide to share
- Recording your decision.

Finally, Annex 3 contains a selection of illustrative case studies where you will find the following example that is especially relevant to social research:

*'A local university wants to conduct research into the academic performance of children from deprived family backgrounds in the local area. The university wants to identify the relevant children by finding out which ones are eligible for free school meals. Therefore, it wants to ask all local primary and secondary schools for this personal data, as well as the relevant children's test results for the past three years.*

• *The DPA contains various provisions that are intended to facilitate the processing of personal data for research purposes. However, there is no exemption from the general duty to process the data fairly. Data about families' income levels, or eligibility for benefit, can be inferred fairly reliably from a child's receipt of free school meals. Parents and their children may well object to the disclosure of this data because they consider it sensitive and potentially stigmatising. Data about a child's academic performance could be considered equally sensitive.*

- *The school could identify eligible children on the researchers' behalf and contact their parents, explaining what the research is about, what data the researchers want and seeking their consent for the sharing of the data.*

- *Alternatively, the school could disclose an anonymised data set, or statistical information, to the researchers.*

- *There is an exemption from subject access for data processed only for research purposes, provided certain conditions are satisfied, for example the research results are not made available in a form which identifies anyone. However, it is good practice to provide data subjects with access to their personal data wherever possible. If subject access is going to be refused, for example because giving access would prejudice the research results, this should be explained to individuals during the research enrolment process'.*

**Appendix 5**

**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 these data are governed by relevant protocols – see 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 5th Principle that the data should not be kept longer than is necessary to fulfil the defined purpose. Once all 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 are 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 is not exempt from the Act. However, the extent to which the university, the student of 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 want 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 are 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)

**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 are 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.