MRS Checklist for Buying and Using Data Lists

August 2015

Reviewed and updated July 2020

MRS is the world's largest association for people and organisations that provide or use market, social and opinion research, business intelligence and customer insight.

MRS
The Old Trading House
15 Northburgh Street
London EC1V 0JR

Telephone: +44 (0)20 7490 4911
Fax: +44 (0)20 7490 0608
Email: codeline@mrs.org.uk
Website: www.mrs.org.uk

Company Limited by guarantee. Registered in England No 518686. Registered office as above.

Table of Contents

Introduction

This Checklist interpret the MRS Code of Conduct (revised 2019) and provides additional best practice guidance. Unless otherwise stated, Checklists are not binding. Their aim is to promote professionalism in the conduct of research, insight and other data processing activities.

The general public and other interested parties are entitled to complete assurance that every project is carried out in accordance with the MRS Code of Conduct and that their rights and privacy are respected.

Rules from the MRS Code of Conduct applicable in each section of this document are stated in bold. These rules are binding on MRS members and MRS Company Partners and breaches may result in disciplinary action. The guidance that follows the rules provides interpretation and additional best practice. Members and Company Partners are reminded that this document is designed to complement the MRS Code of Conduct and should not be consulted in isolation.

As specified in the MRS Code, it is the responsibility of the members to keep abreast of any legislation which could affect their professional activities and to ensure that all those involved in projects are aware of and agree to abide by the MRS Code of Conduct.

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

MRS has produced this checklist to help practitioners act legally and ethically in sourcing participants for research projects. This includes:

- Buying, renting or licensing consumer data lists for research or marketing purposes
- Using client supplied databases or samples such as lists of consumer names, email or postal addresses, or telephone numbers sourced from documents such as their customer purchase and application forms
- Collating details from online data collection processes or social media processes

Researchers can use the questions in this checklist to assess whether personal data such as contact details of potential research participants have been properly sourced. The checklist should be used along with the MRS Code of Conduct and Guidelines.

The Principles of the MRS Code of Conduct

MRS Members shall:

1. Ensure that their professional activities can be understood in a transparent manner.
2. Be straightforward and honest in all professional and business relationships.
3. Be transparent as to the subject and purpose of data collection.
4. Ensure that their professional activities are not used to unfairly influence views and opinions of participants.
5. Respect the confidentiality of information collected in their professional activities.
6. Respect the rights and well-being of all individuals.
7. Ensure that individuals are not harmed or adversely affected by their professional activities.
8. Balance the needs of individuals, clients, and their professional activities.
9. Exercise independent professional judgement in the design, conduct and reporting of their professional activities.
10. Ensure that their professional activities are conducted by persons with appropriate training, qualifications and experience.
11. Protect the reputation and integrity of the profession.
12. Take responsibility for promoting and reinforcing the principles and rules of the MRS Code of Conduct

Definitions

Definitions from the MRS Code of Conduct

Anonymisation:
Anonymisation is the process of removing, obscuring, aggregating or altering identifiers to prevent the likely identification using reasonable means of the individuals to whom the data originally related.

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

Data:
Data is information collected in any nature or format.

Data Collection Process:
A data collection process is any process used to obtain information from or about participants. It includes, but is not limited to, analytics tools, algorithms, interviews, as well as passive data collection.

Member:
A Member is an individual who has been admitted to Membership of MRS in one of the categories set out the MRS Articles of Association.
Note on Definition: *For the purposes of applying this Code, an organisation that has signed the MRS Company Partner Service Quality Commitment that applies throughout the organisation/department/team shall be treated as a Member*.

Participant:
A participant is any individual or organisation from or about whom data are collected.

Research:
Research is the collection, use, or analysis of information about individuals or organisations intended to establish facts, acquire knowledge or reach conclusions. It uses techniques of the applied social, behavioural and data sciences, statistical principles and theory, to generate insights and support decision-making by providers of goods and services, governments, non-profit organisations and the general public.

Definitions from the General Data Protection Regulation used in the MRS Code of Conduct

Consent:
Consent means any freely given, specific, informed and unambiguous indication of a participant's wishes by a statement or by a clear affirmative action, which signifies agreement to the processing of their personal data.

Controller:
Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject:
Data subjects are identified or identifiable living individuals to whom the personal data that is held relates.

Processor:
Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Personal Data Processing:
Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Pseudonymisation:
Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

Special category data:
Special category data means the processing reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union Membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Third party:
Third Party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

The MRS Code of Conduct

The following rules from the MRS Code of Conduct are directly relevant to buying and using data lists.

1. Members must ensure that their professional activities conform to the national and international legislation relevant to a given project, including in particular the Data Protection Act 2018 in the UK, the EU General Data Protection Regulation 2016, and any amendments and superseding legislation that may be enacted. This also covers other applicable legislation inside and outside the UK.

   Comment: See Data Protection & Research: Guidance for MRS Members and Company Partners which will be considered when determining if there has been a breach of the MRS Code.

2. Members must ensure that when undertaking direct marketing activities, they adhere to all relevant specific legal and ethical requirements which apply to direct marketing practice.

   Comment: The following practices fall within the scope of direct marketing:

   a) The offering of client goods or services, or vouchers to purchase client goods or services as an incentive, reward or expression of thanks;
   b) The use of promotional language in describing clients in invitations or introductions to projects;
   c) The offering of materials to participants which promote clients or their products and services. This includes referring participants to a client website at the conclusion of a project.
   d) Members may provide information about a client's products or services where it is necessary to avoid adversely affecting a participant. For example, where a sensitive subject has been discussed, Members may provide information on relevant help lines operated by a client.

   See also Information Commissioner's Office (ICO) Direct Marketing Guidance and Direct Marketing Association (DMA) Code

3. Members must ensure that all of their professional activities, whatever the purpose, are conducted in a transparent manner and that their activities promote compliance with privacy ethics and data protection rules.

4. Members must never undertake any activities, under the guise of research, which aim to manipulate, mislead or coerce individuals. This applies throughout the research process including proposal, data collection, analysis and reporting. Examples of this activity include:

    a) Sell or market under the guise of research ('sugging')
    b) Fund raise under the guise of research ('frugging')
    c) Lobby for political purposes under the guise of research ('plugging')
    d) Create false media content and commentary, including social media, under the guise of research (media-mugging).

6. Members must act honestly in their professional activities.

7. Members must not act in a way which might bring discredit on the profession, MRS or its members.

8. Members must take all reasonable precautions to ensure that participants are not harmed or adversely affected by their professional activities and ensure that there are measures in place to guard against potential harm.

12. Members must carry out Data Protection Impact Assessment (DPIA) for specified types of processing prescribed by data and privacy legislation and for any other processing that is likely to result in a high risk to participants.

13. Members must ensure that the rights and responsibilities of themselves, clients, and subcontractors as controllers or processors are governed by a written contract.

    Comment: See Data Protection & Research: MRS Guidance Note on Controllers and Processors.

14. Members must disclose the identity of clients where there is a legal obligation to do so.
    Comment: Transparency is one of the fundamental principles underpinning data protection laws. In line with this an obligation to name a commissioning client may arise in three main scenarios:

    a) Client is controller or joint controller
    b) Client is the source of the personal data
    c) Client is receiving personal data from a research activity

15. Where files of identifiable individuals are used e.g., client databases, Members must ensure that the sources of the personal data is revealed at an appropriate point in the data collection.
    Comment: The identity of the client must be revealed when data collection is undertaken if clients require personal data from a project.

27. Members must ensure that there is a lawful basis for any collection and processing of personal data undertaken as part of their professional activities.

    Comment: See lawful bases for processing data within the MRS Data Protection guidance.

28. Members must take reasonable action when undertaking data collection to ensure all of the following:
    a) that data collection processes are fit for purpose and clients have been advised accordingly;
    b) that the design and content of data collection processes are appropriate for the audience being analysed;
    c) that participants are able to provide information in a way that reflects the view they want to express, including don't know/prefer not to say;
    d) that participants are not led toward a particular point of view;
    e) that responses and/or data collected are capable of being interpreted in an unambiguous way;
    f) that any potential use of the personal data is revealed;
    g) that personal data collected and/or processed is limited to what is relevant; and
    h) that personal data is stored and transmitted by secure means and only accessible to authorised individuals.

38. Members must ensure that any responses given by participants during data collection are deleted if requested by participants, where possible as the personal data is still being processed.
    Comment: Individuals' rights to erasure can be challenged if the processing is based on the public task legal basis. The rights of individuals to request erasure should be considered unless there are overriding legal considerations. In public task cases where erasure is denied, individuals still have a right to object to the processing via the data protection regulators, the ICO.

42. Members must ensure that there is a lawful basis for the further processing of data for a secondary purpose. This may include consideration of:
    a. Links between the original and proposed new purpose/s.
    b. The context in which the data was originally collected (in particular the relationship between participants and the original data collector).
    c. The consequences of the proposed secondary processing.
    d. The existence of safeguards.

45. Members must take reasonable action to ensure that all records are held, transferred and processed securely in accordance with relevant data retention policies and or/contractual obligations.

46. Members must take reasonable action to ensure that all parties involved in a project are aware of their obligations regarding the collection, transfer, retention, security, disposal and destruction of data.

47. Members must ensure that the length of time, or criteria, for retaining personal data is clearly communicated to all relevant parties including participants, sub-contractors and clients.

48. Members must take reasonable action to ensure that the destruction of data is adequate for the confidentiality of the data being destroyed. For example, any personal data must be destroyed in a manner which safeguards confidentiality.

Buying/Renting Data Lists or Using Client Supplied Data Lists or Databases

- ✓ It is possible to buy or rent data list as long as appropriate due diligence is completed. The ICO states that due diligence when buying data includes:
  - Who compiled the data – was it the organisation you are buying it from or was it someone else?
  - Where was the data obtained from – did it come from the individuals directly or has it come from other sources?
  - What privacy information was used when the data was collected – what were individuals told their data would be used for?
  - When was the personal data compiled – what date was it collected and how old is it?
  - How was the personal data collected – what was the context and method of the collection?
  - Records of the consent (if it is 'consented' data) – what did individuals' consent to, what were they told, were you named, when and how did they consent?
  - Evidence that the data has been checked against opt-out lists (if claimed) – can it be demonstrated that the Telephone Preference list (TPS) or Corporate Telephone Preference Service (CTPS) CTPS has been screened against and how recently?
  - How does the seller deal with individuals' rights – do they pass on objections?

- ✓ A reputable third party should be able to demonstrate that the data is reliable.

- ✓ It is advisable to have a written contract in place confirming the reliability of the personal data. The contract should give reasonable control and audit powers.
  - However, it is important to remember responsibility for compliance independently from the existence of a contract.

- ✓ Once obtained the data, it is still necessary to comply with the right to be informed and provide people with transparency information detailing anything they have not already been told.

- ✓ Article 14 of the GDPR contains a list of the information to provide to individuals when their personal data are not collected directly from them, within a reasonable period and at the latest within a month of obtaining their data. These include:
  - details of the categories (types) of the individual's personal data collected (e.g. contact details, interests, ethnicity etc); and
  - the source of their personal data (e.g. the name of the third party, the name of the publicly available source).

- ✓ A data protection impact assessment (DPIA) enables to analyse processing activities and identify and minimise the data protection risks. It is an integral part of the accountability requirements of GDPR. DPIAs are a legal requirement for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping demonstrate accountability and building trust and engagement with individuals. Article 35 of the GDPR requires to carry out a DPIA in case of:
    - systematic use and extensive profiling with significant effects;
    - processing of special category or criminal offence data on a large scale; or
    - systematically monitor publicly accessible places on a large scale.

    The ICO has compiled a list of processing operations where a DPIA is required as these are 'likely to result in a high risk':
    - large scale profiling;
    - data matching;
    - invisible processing – e.g. list brokering, re-use of publicly available data;
    - tracking the geolocation or behaviour of individuals; and
    - targeting children or other vulnerable individuals.
- ✓ The DPIA is a dynamic document to be reviewed and updated to ensure it reflects any changes in the research project. The review process does not stop once processing personal data commences. It should be periodically reviewed at suitable intervals during longer term projects to ensure it remains an accurate assessment of the processing undertaken, the risks and the mitigations in place.

Additional guidance on DPIAs is available from the ICO and the EDPB Guidelines on Data Protection Impact Assessment (DPIA)

Useful questions to ask

- ✓ Who compiled the original list and how?
    - Is it from original sources or another data list broker?
    - Is it from public data, commercial sources or directly from the individual?
    - Are children under 16 screened out?
- ✓ Is the list based on informed consent of individuals?
    - When was consent obtained? Was it based on opt-in or opt-out consent?
    - What information and assurances were individuals given in providing their details? What exactly does their consent cover?
    - Were the uses of the data made clear, in plain English and in easily readable font or language?
    - Was consent given for disclosure only to named parties or to third parties?
    - Did individuals have notice that their information would be shared with third parties?
- ✓ How is the list maintained?
    - When was the list last cleaned?
    - How often is it updated? Monthly, annually?
    - Can individuals correct their details or opt out of the list?
- ✓ How often is the list used?
    - Is it frequently used by list buyers or renters?
    - Is it used primarily for market research or other purposes?
- ✓ Are there any known problems with the list?
    - What reports and feedback have been received? Are there any complaints about the accuracy of the source list?
    - Is there a guarantee that the list has been validly sourced?
    - Have the suppression policies been applied and are they up to date?

Additional Resources

MRS Code of Conduct 2019

Data Protection & Research: Guidance for MRS Members and Company Partners 2019

MRS Guidance Note - Controllers and Processors (PDF) January 2020

MRS GDPR in Brief Series

DMA Compliance Documents and Templates for List Rental

ICO Direct marketing code of practice