MRS Regulations for the Buying of Qualitative Research Recruitment Services

Introduction

Over the years, questions have been asked about whether all qualitative recruiter practices are fully in line with the legal and ethical requirements that underpin research.

This MRS Guideline brings together all the key legal requirements, process standards and MRS Code rules that relate to the practice of qualitative recruitment, to enable MRS Company Partners to understand their corporate obligations in this area. The aim being that by improving understanding, among organisations and individuals that commission qualitative recruitment, will result in more stringent controls being placed upon qualitative practices, to ensure that future recruitment will be fully in line with the legal and ethical requirements.

It should be noted that the MRS rules and standards highlighted in this guidance are those that are generally considered to be most relevant to recruitment practices. However, there are specific rules for certain sectors and disciplines, such as the BHBIA and EphMRA standards for health research recruitment, which should also be adhered to in addition to this guidance.

The Legal Requirements: Data Protection Act 2018

The MRS Code of Conduct is drafted reflecting the legal requirements from the Data Protection Act 2018, and how these impact on the obligations of researchers. However, it is worth stating the legal framework that underpins this, reinforcing how many of the ethical requirements of the MRS Code of Conduct relating to qualitative recruitment are to ensure that recruitment is being conducted in accordance with the Data Protection Act 2018.

Explanation of Key Terms

Child: a child is an individual under the age of 16.

Controller: Sometimes called a "Data 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 Protection Act 2018: The Data Protection Act 2018 is an Act of Parliament which defines UK law on the processing of data on identifiable living people. The Data Protection Act controls how personal information is used by organisations, businesses, or the government.

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

Joint Controller: is where two or more controllers jointly determine the purposes and means of the processing of the same personal data.

Personal data: means data that is wholly or partly by automated means; or the processing other than by automated means of personal data which forms part of, or is intended to form part of, a filing system. Personal data only includes information relating to natural persons who can be identified or who are identifiable, directly from the information in question; or who can be indirectly identified from that information in combination with other information.

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.

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

Recruiter: means a person or organisation which sources and recruits participants for in market and social research activities. Recruiters are used mainly for qualitative research e.g. recruitment of participants for focus groups, depth interviews, ethnographic research, UX testing, etc.

Sensitive Personal Data - Special category data (sometimes called sensitive data as it needs more protection when it is being collected) means personal data about an individual's (a 'data subject'):

race
ethnic origin
politics
religion
trade union membership
genetics
biometrics
health
sex life
sexual orientation

In particular, this type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination. In addition, there are separate safeguards for personal data relating to criminal convictions and offences, or related security measures, and largely the same conditions apply to this data as with special category data.

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 rules for using personal data in the Data Protection Act 2018

The principles of the Data Protection Act 2018 are that data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Key Legal Requirements

Contracts and Fee

The guiding "construct" underpinning the 2018 Act can be summarised as that of "informed consent" which comprises two key components in terms of the fundamental rights of individuals being asked for or providing information about themselves:

Core Concepts of Data Protection Act 2018 and GDPR are:

Transparency: being transparent about what is happening in any process. For research recruitment transparency requirements apply:

- When gathering consent, you need to meet the higher threshold for demonstrating consent-based research
- Effective communication and clear information, for example with privacy consents, ensuring the language is appropriate for the audience whose personal data is being collected e.g. children, vulnerable adults, etc.
- Procedures for allowing participants to exercise their rights such as subject access rights, withdrawing consent and having procedures in place to enable these rights to be easily managed and implemented
- Respect of data subjects, participants, is a core requirement

Accountability: being able to demonstrate you have taken responsibility for all data protection measures. Accountability principle applies to all irrespective of size, although how you implement requirements will be scalable. Examples of accountability requirements include:

- Detailed written records are important, although the responsibility of this is likely to be shared with others involved in any research project e.g. field agencies, clients and so on.
- The privacy legislation is a risk-based piece of legislation. If you have low-risk small amounts of personal data, your risk is likely to be less than those who have large datasets
- Mandatory breach notification
- The appointment of a Data Protection Officer is only mandatory for those that process large scale personal data, collect high levels of special category data or undertake large scale monitoring of individuals. It is unlikely that recruiters will need a Data Protection Officer although organisations that offer recruitment services may need to.

1. The Data Protection Act 2018 will <u>always</u> apply for any qualitative recruitment exercise.

2. Participants are data subjects, information collected during a recruitment exercise is personal data, Recruiters and Company Partners will be either Data Processors or Data Controllers and will have obligations under the Act as a result.

3. When Recruiters and/or Company Partners create databases of participants or decide how or why personal data will be processed, they will be Data Controllers.

4. When Recruiters and/or Company Partners are following instructions determined by clients and have no ownership or right to subsequently use any data gathered they will be a Data Processors of the collected data.

5. Data Controllers must pay and annual fee to the Information Commissioner's Office, setting out the purposes for which they process personal data (replaces the process of 'notification' from the 1998 Act).

6. Company Partner and Recruiters must gain informed consent which means that participants are informed from the outset the information being collected, its purpose (e.g. for research), and, if further information is likely to be necessary. See rule 31 of the MRS Code of Conduct for full details of the requirements

7. Company Partners must ensure that recruitment documentation clearly states all relevant information that participants would require to decide as to whether to participate in a project, for example:

   - Purpose of the recruitment
   - Location, time and duration of the activity
   - Type of research activity e.g. group, depth, paired depth, on-home, etc.
   - Client (if identified)
   - Monitoring, observation or recording arrangements
   - Incentives (and any terms or restrictions that might apply to incentives)
   - Any unusual and/or unexpected activities which might be asked of participants during the qualitative project e.g. pre- or post-tasks, physical activities during a group, etc.
   - Re-contact (if applicable)

8. Company Partners and Recruiters must ensure that permission for re-contact is obtained either during the initial recruitment interview or during the subsequent research. It cannot be obtained post-research.

9. Company Partners must have recruiter monitoring processes in place to ensure that informed consent principles are being adhered to.

10. Company Partners must ensure that only accredited recruiters and/or RAS Accredited Companies are used to supply research recruitment services unless specific and identified circumstances or geography prevent this. This requirement will apply from 31st March 2021 at which time there should be sufficient accredited recruiters to enable Company Partners to meet this requirement.

11. Company Partners must either stop using Recruiters who fail any recruiter monitoring processes and/or have any specific issues addressed before using Recruiters' services further.

    Note: Company Partners may be held responsible for illegal and/or unethical recruiter activities if inadequate steps are undertaken by the Company Partner. Appropriate steps may include briefing instructions for Recruiters, spot checks and so on.

Data Use

12. Company Partners must check the source of any data being used or supplied for recruitment. This would include data collected or supplied by Recruiters. If a Company Partner has any doubts as to whether participant names and contact details have been collected legally, they must not use the information.

13. Personal data collected from participants for a specified purpose, for example as part of recruitment for research projects, cannot be used for other purposes. This would include, for example, building participant recruitment databases. Such activities can only be conducted if participants agree for their data to be used in this way, and the activities are authorised by the terms and conditions which underpin the exercise.

14. When personal data is collected from participants for recruitment only data that is necessary for the project must be collected. To gather additional information would be excessive and in breach of the data minimisation requirements set out in the Data Protection Act 2018. MRS Company Partners must ensure that the data collection techniques used to recruit participants only collect information required by the research.

15. Company Partners must ensure that instructions regarding personal data collected during recruitment are being adhered to. For example, ensuring that Recruiters are not retaining identifiable participant information, for future recruitment, without permission from the participants and only if in accordance with the existing terms and conditions which underpin the exercise.

    Note: to meet this obligation Company Partners should consider the following steps:
    - *Standards contracts/terms of engagement with Recruiters, which clearly specify what the Recruiters can and cannot do with data they received (e.g. if recruiting from client lists) or that they collect in the course of undertaking research on behalf of an organisation.*
    - *Financial penalties, specified in the contract, for any Recruiters found to have used or collected data outside of contracted terms.*
    - *Spot checks of participants post-projects (particularly those using client lists and/or with re-contact questions) to ascertain if they have been re-contacted by Recruiters.*

Data Accuracy

16. Company Partners and Recruiters must ensure that any retained personal data provided by participants is kept accurate and up to date as required by the data accuracy requirements of the Data Protection Act 2018. This would include recruitment databases gathered with permission from participants.

Data Security, Retention and Destruction

17. Any personal data held by a Company Partner and Recruiters (including paper, digital, audio/visual recordings) must be kept secure and only those with appropriate authority should be able to access personal data. For Company Partners these obligations apply to all personal data, whether held by the Company Partner or by subcontractors, workers or third parties working on their behalf.

18. Company Partners and Recruiters must not keep personal data for longer than is required to fulfil its research purpose.

19. Company Partners and Recruiters must have data security, retention and destruction policies/protocols in place and being adhered to, to ensure that excessive data is not being retained and all contractual obligations are being met (this may include clients' post-research data requirements). This includes any personal data that might be held with data processors, subcontractors, freelancers, Recruiters, etc. that have retained personal data for the completion of a project.

    Note: Company Partners should consider what checks they can undertake to ensure adherence to these requirements. For example:
    - *Spot checks of Recruiters procedures.*
    - *Include mystery shopper contacts in data sets supplied to Recruiters to see if Recruiters are correctly following corporate procedures and protocols. For example, if procedures are not being followed mystery shoppers may be contacted after a sample should have been destroyed following a recruitment process.*
    - *Obtain documentary evidence of the destruction of manual files, etc. from Recruiters (e.g. confidential shredding invoices).*

20. Company Partners must ensure that Recruiters meet any requests for the deletion of participant data including responses obtained during recruitment.

    Note: This might be achieved by asking for confirmation and/or evidence of deletion, obtaining a signed statement from the recruiter that information has been deleted, etc.

Data Access

21. Data Subjects e.g. participants, have the right to access any personal data held about them. The right of subject access applies to all personal data files including digital files, recordings from groups and potentially paper/manual recruitment documentation. Company Partners and Recruiters must respond to any subject access requests received.

Key Ethical Requirements

The MRS Code of Conduct mirrors the legal requirements already identified. However, there are additional requirements, specific to the MRS Code of Conduct.

Honesty

1. Company Partners and Recruiters must act honestly in their professional activities.

2. When Company Partners retain Recruiters to undertake work on their behalf, Company Partners must ensure that Recruiters are being honest (i.e. are not intentionally deceiving participants) in their working activities. If there is any doubt about the veracity of Recruiters' practices these must be honestly disclosed with relevant parties e.g. clients, MRS.

3. Company Partners must also be honest in their dealings with clients, recruiters, participants, etc.

4. Company Partners must honour any assurances made, such as payment of incentives including assurances as to when payment will be made and must not pass this burden onto Recruiters.

5. Company Partners and Recruiters must conduct research recruitment honestly without misleading either those that retain their services or those they approach for research or interview purposes.

6. Company Partners must ensure that participants are able to confirm the bona fides of any Recruiters used by them, including relevant contact details.

   Note: This could include for example, providing Recruiters with IID cards (MRS or other), to be used when working on behalf of a Company Partner.

7. Company Partners that use Recruiters must check that Recruiters are undertaking recruitment legally and ethically. Company Partners must monitor and check processes and procedures using a systematic, structured formal process to ensure Recruiters are operating appropriately.

Harm

8. Company Partners and Recruiters must take all reasonable precautions to ensure that participants are not harmed or adversely affected by their professional activities.

   Note: Harm is a broad concept and could, for example, include financial, legal, physical or emotional harm.

   Increasingly, Company Partners are requesting participants prove their credentials when participating in research, to ensure that specification requirements are being met, and to alleviate 'fraudulent participants'. If participants are recruited poorly it is possible that harm could result i.e. if an individual has unknowingly (as opposed to knowingly) been mis recruited. The harm might be embarrassment, loss of incentive, cost of attending the group, etc.

9. Company Partners should ask key questions to determine whether research activities might cause/d harm to participants.

   Note: For example, if you had a participant who arrived late for a group – should an incentive be paid? Some questions you could ask to determine the answer:

   - *Did the participant incur any financial costs to travel to the group location?*
   - *Did the participant have to travel a long distance to attend the group?*
   - *Did the participant have to travel a long time to attend the group?*
   - *Where there external factors that limited the participants ability to arrive on time e.g. travel disruption, tube strike?*

   If the answer to the above questions is yes, then some form of financial harm would result from no financial reimbursement. Company Partners should set out prior to recruitment any conditions which might limit payment of incentives e.g. late arrival, so participants understand the terms for their participation and misunderstanding are less likely to occur.

10. Company Partners and Recruiters must communicate clearly to participants the consequences of agreeing to participate in a research exercise, for example, confirmation of participant identities, if physical activities are part of a group activity or observers are to be present. Company Partners must ensure that such relevant information is clearly detailed in any instructions to Recruiters and Recruiters must ensure that this information is relayed to participants during recruitment.

    Note: There are a variety of methods for confirming identities. The evidence used must be creditable third-party evidence such as passport, drivers licence, and other photo IDs (e.g. Validate UK and other such schemes). In rare cases it may not be appropriate to check ID documentation, if this is the case detailed reasoning must be documented including other methods used to confirm participant identities.

Recruitment of Children

11. Recruitment of children for qualitative research is a specialist area, and Company Partners should only use Recruiters who have appropriate knowledge and experience to do this type of research.

12. Company Partners must provide detailed instructions to Recruiters to ensure any recruitment of children is conducted in accordance with the MRS Code rules.

Key Process Requirements - ISO 20252:2019 and IQCS

The IQCS standards are a sub-set of the Fieldwork rules (detailed in Annex B) of the ISO 20252:2019 for Market, opinion and social research including insights and data analytics standard.

The following information has been extracted from the ISO standard, but applies whether organisations are IQCS or ISO 20252:2019 certified.

Unlike Sections 1 and 2, the following requirements **must** only be followed by Company Partners that are also either IQCS or ISO 20252:2012 certified. However, all Company Partners are obliged to adhere to the MRS Quality Commitment, which places obligations on Company Partners to have adequate quality procedures to meet their legal and ethical requirements. As such the following procedures will be relevant for all MRS Company Partners.

ISO 20252:2019 Definitions

Fieldworker: person involved in the collection of data for market, opinion and social research

Note 1 to entry: Fieldworkers include, but are not limited to, face-to-face and telephone interviewers, recruiters for qualitative or other research, "mystery shoppers" and other people carrying out data collection by observation, and persons collecting data from retail outlets, following instructions from the service provider

Based upon the above definition, **all** fieldworker requirements within the ISO standard would also apply to Recruiters. However, in practice this has not been the case and only those elements which specifically identify "Recruiters" are applied.

This guidance will only look at the mandatory requirements (in grey boxes), not the wider requirements regarding interviewers. It should be noted however, that to be in strict accordance with the definition set out in ISO 20252 other sections of the standard could apply.

Recruiter Identification

Fieldworker identity document (ID) – clause B.3

The service provider shall issue fieldworkers conducting face-to-face interviewing with an identity document (ID), preferably including a photograph. The ID shall include the validity period (e.g. the date of issue and the expiry date, year during which the ID is valid), and the name and contact details of the entity (e.g. the service provider, the fieldworker) to whom it belongs.

1. It is good practice for Company Partners to ensure that Recruiters working on their behalf have some form of identification, which could be, for example, an MRS ID card.

Participant Recruitment and Validation

Respondent recruitment – clause B.6.3

The service provider shall ensure that the primary aim of validation of participant recruitment is to confirm demographic and other recruitment criteria of participants and the work of fieldworkers, and to avoid participant participation in excess of what is specified in research proposals.

Where participants are recruited by fieldworkers (e.g. face-to-face, telephone), the service provider shall validate their work as specified in B.7, according to the required validation levels. The service provider shall ensure that validation methods include re-contact or monitoring (e.g. for telephone recruitment from central locations). The service provider shall ensure that validation is carried out; this can be before, during, or after qualitative data collection. The service provider shall take action where discrepancies are found.

NOTE 1 Validation by re-contact can be conducted during qualitative data collection. In such cases, self-complete or self-administered validation questionnaires can be used provided they are administered by individuals who were not involved in the original recruitment.

NOTE 2 In some cases, the only criterion for recruitment is that the participant is included in a recruitment list (e.g. customer lists). In such cases, validation can be limited to ensuring that recruited participants were indeed on the list, and re-contact or monitoring can be considered unnecessary.

Where participants are recruited online, including from access panels, the service provider shall ensure that validation is carried out as specified in Annex E. In online situations where recruitment and validation are conducted by the same people, the service provider shall ensure that validation records are available to moderators.

The service provider shall confirm identities and exclude "professional" participants at qualitative interviews/group discussions by using appropriate participant documentation. Moderators shall also confirm participants meet relevant recruitment criteria. The service provider shall determine how identities are confirmed and how moderators are to confirm they match to recruitment criteria.

2. Company Partners must ensure that correct information is stated on recruitment documentation as to the sources of participant recruitment. If there are doubts as to the legitimacy of how participants have been recruited, for example from a recruiter database that has been compiled illegally, Company Partners must not use the participant information nor any resulting research outputs.

Respondent recruitment validation (Clause 5.5.2)

The primary aim of validation of respondent recruitment shall be to confirm the demographic and other recruitment criteria of respondents and the work of fieldworkers.

Where respondents are recruited by fieldworkers (face to face or by telephone) their work shall be validated as per 5.4 including the required validation levels specified in 5.4.3. Validation methods may include re-contact or monitoring (e.g. for telephone recruitment from a central location). Such validation may be carried out before, during or after the qualitative data collection. The need for action to be taken where discrepancies are found applies as per 5.4.1. Validation records shall be prepared in accordance with 5.4.4.

NOTE: Validation by re-contact can be conducted during qualitative data collection. In this case a self-completion or administered validation questionnaire can be used but should be administered by someone other than the original recruiter.

NOTE: In some cases the only criterion for recruitment can be that the respondent is included in a list from which respondents are to be recruited (e.g. a customer list). In this case validation need be no more than ensuring recruited respondents were on the list and re-contact or monitoring can be considered unnecessary.

3. Recruitment validation is a useful and necessary procedure for confirming participant contact and details. Company Partners should also consider how this process might be used to address other obligations such as assessing recruiter behaviour and practices during participants' recruitment, etc.

Data Collection Records

Participant reassurance, invitations and data collected from children or vulnerable persons (clauses 4.1.2.2, 4.1.2.3, 4.1.2.4, 4.1.3.2 and 4.1.3.3)

Invited or recruited participants shall be informed by the service provider that participation is voluntary.

The service provider shall ensure that participant reassurance occurs:

a) during each recruitment or invitation, regarding the types of personal data, proposed uses, and retention and/or reuse of the data to be collected
b) during direct data collection (e.g. face-to-face, telephone) regarding confidentiality principles, purposes for which the data may be used, and identity and contact details of the service provider and any subcontractors and/or client(s), as appropriate.

Where digital identifiers (e.g. cookies) are used by the service provider during data collection, this shall be communicated to participants including the purpose of the intended identifiers.

Whenever geo-location or geo-fencing methods are to be used to collect participant data, the service provider shall make participants aware of this and obtain consent.

Where there is no direct contact between the service provider and the participant/s and it is not possible to provide direct assurances, privacy obligations shall still be met.

Reasonable precautions shall be taken by the service provider to ensure that participants and observed people (including those who may not be aware they are being observed) are not identified, harmed, or adversely affected as a result of their participation.

The service provider shall provide each potential participant invited to take part in a research project with appropriate information, including:

a) a general description of the purpose of a project;
b) the estimated length of their participation time;
c) a statement of the confidentiality of each participant's responses;
d) a statement of the anonymity and/or identification of each participant's responses;
e) the closing date for completed responses (if applicable);
f) full disclosure of incentive terms and conditions related to the project;
g) information as to whether the invitation is sent out on behalf of another service provider; and
h) the opportunity to unsubscribe or opt out of the research activity.

Where participants ask for the above details of a project, if the information cannot be shared prior to participation, the service provider shall share these details after participation.

When collecting data from children or participants considered to be vulnerable, the service provider shall:

a) obtain consent from a parent, guardian, or responsible adult after providing them with sufficient information about the research process;
b) exercise due care during the data collection process including the child's or vulnerable person's agreement to participate.

Due care may include additional training of fieldworkers and additional fieldworker guidelines.

Where permission to collect data from children and vulnerable persons has been obtained, the permission shall be renewed at least every 12 months or at the next invitation to participate, whichever is most frequent.

Definitions of what constitutes a child, vulnerable person, and responsible adult vary from country to country and this shall be taken into account in multinational research.

Specific project research records that are required to enable project traceability and replicability shall be retained for a minimum of 24 months or as agreed by the client.

Project records traceability and replicability refers to records held by the service provider and any subcontractors used.

Additionally:

a) primary records shall be retained for 12 months or as agreed by the client;
b) data used to identify participants shall be retained for any necessary administration and/or quality control period or as agreed with the participant/s.

The extent and nature of records management, including maintaining, archiving, and destruction of records for research activities undertaken by the service provider, shall be:

a) controlled in a secure manner to the extent necessary to support the requirements of the standard;
b) protected from loss of confidentiality, privacy, and security as prescribed in the standard; and;
c) protected from improper use and loss of integrity as prescribed in the standard.

4. Company Partners must ensure that they have adequate recruiter procedures and protocols in place to ensure that relevant records are retained and retrievable for all research projects undertaken.

5. Company Partners must ensure that when subcontractors are used for qualitative recruitment this information is recorded against the project file.

6. Company Partners must balance the data collection requirements of ISO 20252:2019 with the broader requirements of the MRS Code and the Data Protection Act regarding retention, security and destruction of data. Personal data once used, and which is no longer required for client, audit or certification purposes must be securely destroyed as soon as it is feasibly possible.