BHBIA

BHBIA Ethics & Compliance

Preparing for the General Data Protection Regulation

Consents for Market Research

What is required and when

Introduction

This guide provides detail upon the different consents that might be required during the course of a primary market research project and at what stage these consents must be secured, before or during fieldwork.

The guidance takes account of General Data Protection Regulation (GDPR) requirements. It complements the BHBIA's guide '*GDPR – Legal Grounds for Data Processing*' available on the BHBIA website.

The BHBIA's Ethics & Compliance Committee is providing this guidance as general information for its members. It is not legal advice and should not be relied upon as such. Specific legal advice should be taken in relation to any specific legal problems or matters. Whilst every reasonable effort is made to make sure the information is accurate, no responsibility for its accuracy or for any consequences of relying on it is assumed by the BHBIA. We do expect to update our guidance on the GDPR as more information becomes available.

Consent

The following bullet points summarise BHBIA's guidance on Consent and are drawn from *GDPR – Legal Grounds for Data Processing,* see Appendix 1 on page 6 for the full details.

- Consent must be given by a clear affirmative action
- Consent must be freely given, clear, obvious and informed
- To secure consent to process personal data for MR, potential respondents must be told
  - Who is collecting the data and who is going to share it
  - Why - for what purpose
  - Any other information required to make an informed decision

  See Appendix 1, page 7 for more specific detail.
- Consent is always specific to a single purpose
  - Personal data can only be used for the purposes for which it was collected
  - If you pass on personal data to colleagues inform them of the purpose(s) for which it can be used
- Explicit consent is necessary for processing special category (sensitive) personal data such as health data, automated decision making or overseas transfers to countries without adequate safeguards. Explicit consent must be confirmed in a clear and specifically worded statement.

- Consent or refusal must be recorded
- Individuals can withdraw their consent any time they want to and It must be as easy to withdraw consent as it was to give it

Naming Data Controllers

- GDPR requires that data controller(s) relying on consent are named at the time that personal data is obtained as part of the MR process.
- **If the end client company is a data controller i.e. determining the purposes and means of processing personal data (either alone or jointly with another data controller) their identity must be shared with the data subject.**
  - Remember the end client is a data controller if data processing carried out by a joint controller or processor (e.g. an agency) is taking place for the end client's overall purpose. This is the case even if the end client never accesses any personal data.
- IF naming the end client before the interview would undermine the integrity of the work, this may be done at the end of the interview BUT:
  - Respondents must be made aware at recruitment that:
    - the client will be named at the end of the interview
    - they can withdraw their consent at any point
  - If the end client is receiving personal data they must be named before any transfer takes place
  - The justification for this should be documented

This guidance is consistent with MRS's guidance on this issue available within section 4.2.6 of the MRS Guidance on Data Protection & Research 2018 available on the MRS website http://www.mrs.org.uk/pdf/MRS%20Data%20Protection%20and%20Research%20Guidance%20Section%201%20_28.04.2018.pdf. Section 4.2.6 is reproduced in Appendix 2 on page 10 of this document.

The BHBIA is liaising with both the MRS and the ICO to make sure the guidance is consistent with GDPR and DPA 2018 requirements. There may be additional guidance on this issue to come and so members should be aware that the advice above is subject to change.

What consents might be required and when

Abbreviations used:

AE Adverse event (including adverse reactions, product complaints, special reporting situations)
MAH Marketing authorisation holder
MR Market research
PV Pharmacovigilance

Before fieldwork – at recruitment	
Consent	***Explanation***
To participate in MR	*Informed consent is a process by which a participant voluntarily confirms his or her willingness to take part in a particular project, after having been informed of all aspects of the project that are relevant to their decision to participate.* MRS Code of Conduct, September 2014
To data processing for the purpose of MR	*Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.* General Data Protection Regulation, Article 4
To process personal data not available in public domain	To process personal data that's not freely available in the public domain (e.g. to use a list of detailed doctors for sampling provided by the commissioning client company), the list holder must have a lawful basis for this, and consent could be the lawful basis used.
To interview a child	Explicit consent must be given by the child and the child's adult guardian to approach a child to ask them to participate in MR.
To install and use software	To install and use software, such as an app to gather personal data, the individual must be informed of the purpose of the software, the type of data it collects and any impact it will have on the device's functioning or performance e.g. reducing battery life and consent to this.
To add individuals to an influencer mapping exercise	To collect individuals' personal data for an influencer mapping exercise, there must be a lawful basis for the data processing, the lawful basis could be consent although this may not be practical and another basis, such as legitimate interests could be used.

Before fieldwork – at recruitment *continued*	
Consent	***Explanation***
For the agency to observe or record non-anonymised fieldwork for analysis purposes	Even if it's only for analysis by the agency acting as a data processor, the BHBIA's Legal & Ethical Guidelines require that anyone being observed or recorded must be told why and who will listen to/see it (agency name) and agree to this, irrespective of how it will be viewed or recorded e.g. via one way mirror or video-streaming. If in doing this personal data is processed data protection requirements mean that if the agency and/or end client is a data controller they must be named. Similarly if the agency and/or end client is the source of or a recipient of the personal data they must be named. The client's identity may be disclosed at the end of the interview IF naming the end client beforehand would undermine the integrity of the MR BUT: – Respondents must be made aware at recruitment that: - the client will be named at the end of the interview - they can withdraw their consent at any point – The justification for this should be documented
To allow the end client to observe or listen in to non-anonymised fieldwork live	**By one-way mirror or sitting in** – you must tell respondents that the end client will observe them and respondents must consent to this beforehand. – In this situation personal data isn't being transferred to the end client, so data protection legislation does not apply and so the end client may remain anonymous unless you are legally obliged to reveal their identity for another reason e.g. the end client is a data controller or the end client supplied the sample. If there's no contrary legal obligation. – Before fieldwork starts, you should agree and document the client position on whether you can reveal their identity to respondents and if it can be revealed, when – during or at the end of the interview. You should reflect this in screener and interview materials, so that interviewers can react appropriately. **Live viewing – via video relay/streaming, with and without recording** - Data protection requirements mean you must name the organisation(s) viewing as part of informed consent for this purpose before transfer of the personal data takes place. So if for example, the end client is viewing fieldwork live via a video-stream the client's identity must be revealed before fieldwork as part of the information communicated to secure respondents' informed consent for this.
To allow the end client to observe or listen in to non-anonymised fieldwork <u>after</u> fieldwork	**Delayed viewing – via video relay/streaming, with and without recording** - If the end client wants to view or listen in to fieldwork after it has taken place, consent for this must be secured before the interview but the client's identity may be disclosed at the end of the interview (before any personal data is shared with the client) IF naming the end client beforehand would undermine the integrity of the MR BUT: – Respondents must be made aware at recruitment that: - the client will be named at the end of the interview - they can withdraw their consent at any point – The justification for this should be documented

An example to illustrate data protection requirements when fieldwork is recorded and consent is sought for viewing by the end client:

- An end client (a pharmaceutical company) commissions MR and is a data controller
- A MR agency designs the MR, moderates a series of group discussions and is a data controller
- A fieldwork agency recruits the groups and is a data processor

If the end client wants to view non-anonymised fieldwork via video-streaming to their offices:

- live – the end client must be named before fieldwork begins and any personal data is transferred, irrespective of any concerns about whether this would impact the integrity of the MR findings
- after fieldwork has taken place – the end client may be named at the end of fieldwork before any personal data is shared with the end client if there is a genuine concern that identifying the end client would impact the integrity of the MR findings

During fieldwork - at the end of the interview	
The following consents may be secured at the end of the interview as consent for these tasks is not essential to participation in the MR. These tasks can be considered separate processing operations.	
Consent	***Explanation***
To forward personal data in an AE report	If personal data is collected whilst an adverse event report is being compiled, consent to forward that personal data to the MAH's PV department for possible AE follow-up is required.
To forward personal data if disclosure is required	ABPI Disclosure UK requirements mean that incentives paid to individual HCPs participating in MR must be disclosed by client companies if the client company knows the identity of the HCPs. HCPs must give their consent for their personal data to be disclosed (if they don't anonymised information is disclosed).
To add individuals to a database for a non-MR purpose	If data originally processed for MR is to be processed for a second and non-market research process, separate consent for this is required. MR must be clearly separated and distinguished from non-MR purposes.
To re-contact a respondent after fieldwork	To re-contact a respondent after fieldwork, their consent for this must be obtained during recruitment or fieldwork. Respondents must be told why they might be re-contacted and who would contact them (organisation and roles, not names).
To keep respondent details on file for future MR	To keep respondent details on file to contact them about taking part in future MR, respondents must agree to being re-contacted and to their personal data being held on file for this purpose.
To use non-anonymised MR output for non-MR purpose	If non-anonymised MR output is to be used for a non-MR purpose e.g. film footage showing respondents faces taken from a group discussion is to be included within a training film, consent for the non-MR use of the output is required.

APPENDIX 1

Source: ***GDPR – Legal Grounds for Data Processing*** available on the BHBIA website on the GDPR page.

Consent for Data Processing

The GDPR definition of consent is similar to but a little more detailed than the Data Protection Directive definition. Consent under GDPR refers to:

> "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*"

Consent must be:

- Given by a **clear affirmative action** e.g.
  - Signing a written statement
  - Answering yes to an oral request
  - Ticking/checking an opt-in box online or on paper
  - Clicking an opt-in button or link online
  - Selecting from (equally prominent) yes or no options
  - Choosing technical settings or preference dashboard settings
  - Responding to an email requesting consent
- **Freely given –** consent wouldn't be considered freely given if there is a clear imbalance of power between the person or organisation requesting consent and the data subject, so that if for example doctors are involved in the recruitment of patients for a MR exercise, great care must be taken that the patient does not feel undue pressure to participate simply because they were asked by a doctor.
- **Specific** (to a single purpose), different data processing activities should have separate consents e.g. consent to store individuals' personal data on a database, consent to video record their participation in a group discussion for analysis, consent to share this with the commissioning client. If securing separate consents would be unduly disruptive or confusing it may not be necessary but as a minimum, consent must specifically cover all purposes. Thinking ahead and anticipating potential uses of the data will allow you to secure all the consents you could need.
- **Clear** – unambiguous, concise and easy to understand, using simple and clear language.

  It is possible to 'layer' the information i.e. provide it in chunks in a step wise fashion e.g. tell respondents they have a right to withdraw in the consent statement, tell them how this can be done in the privacy policy and provide the privacy policy as a separate document or online.
- **Prominent and obvious**, not 'bundled up' with other terms and conditions
- **Verifiable** – you must be able to demonstrate that someone has consented
- **Informed**

- **If personal data are to be obtained directly from an individual** e.g. via a MR interview, the information overleaf must be delivered when it's obtained i.e. at recruitment.
- **If the personal data are <u>not</u> obtained directly from the individual** e.g. via digital listening or from a customer database, the information overleaf must be delivered:
  - When the first communication takes place If the data are to be used to communicate with an individual
  - If the data are to be shared/disclosed before this happens.

To be informed it must include:

- ✓ **Name and contact details of the data controller(s)** and where applicable the data controller's representative and the data protection officer
- ✓ **The recipients or categories of recipients of the personal data** e.g. the name of the commissioning client if they are to be given access to non-anonymised recordings of respondents participating in MR
- ✓ **Legal basis for processing**
- ✓ **Purposes** of the processing – why you want the data
- ✓ **Types of processing activity** – what you will do with the data
- ✓ **Where processing is based** and **details of any data transfer to countries without adequate data protection** (generally countries outside the EU)
- ✓ **How long the data will be stored** or if that's not possible, the criteria used to decide this
- ✓ **Right to withdraw consent** at any point and other rights - to have their personal data rectified or erased, to access or move their data, to restrict or object to data processing in future and to complain to the data protection authority (the ICO in the UK) - some of the detail could be put in to the privacy notice. It must be as easy to withdraw consent as it was to give it, so it should be an easily accessible single step. It is good practice to tell individuals how to withdraw.
- ✓ **Existence of any automated decision making** and its consequences
- ✓ **Contact details of data protection officer** where applicable

In addition, when the data is not obtained directly from the individual, the data subject must also be informed of:

- ✓ The **categories** (types) of personal data to be collected
- ✓ The **source** of the personal data

Researchers and analysts need to provide all the information above to secure consent under GDPR requirements and they must also provide the information detailed within the BHBIA's Guidelines (e.g. the methodology, duration of fieldwork, reimbursement offered etc.). For

further details see section E4.2 and E6.1 of the BHBIA's Legal & Ethical Guidelines, available on the BHBIA website - www.bhbia.org.uk

Explicit consent

Explicit consent is not clearly defined within the GDPR but it is basically a slightly higher standard of consent and is necessary for:

- Processing special category (sensitive) personal data such as health or financial data. There are other ways to legitimise processing special category data but these are unlikely to apply to MR and data analytics.
- Automated decision making including profiling (profiling under the GDPR refers to the use of an individual's personal characteristics of behaviour (e.g. for the purposes of direct marketing). Profiling is not the same as segmentation.
- Overseas transfers to countries without adequate safeguards.

Explicit consent must be confirmed in a clear and specifically worded statement (oral or written), so signing a statement would be explicit consent but an affirmative action alone such as responding to an email requesting consent would not be explicit consent. The ICO advise that if you need explicit consent, you take extra care with the wording. The following example helps to explain the distinction:

✘ *We will provide* [the client] *with film footage of the group discussion to help them understand the market research better* – this is not explicit consent

✓ *I consent to you providing* [the client] *with film footage of the group discussion to help them understand the market research better* – this is explicit consent

Consenting children into MR

BHBIA and MRS guidelines currently require you to secure parental consent to approach a child to ask for their consent to participate in MR if the child is under 16. The GDPR requires parental consent for children under 16 to use online services provided at the user's request ("information society services"). The 2018 UK Data Protection Act is likely to lower this age to 13. If you rely on children's consent, you must have age-verification measures in place, and make 'reasonable efforts' to verify parental responsibility.

Keeping records of consent

The GDPR requires you to keep records of the consents secured. Your records should include:

- **Who** consented – the individual's name or other identifier (e.g. online user name, session ID)
- **When** they consented – a copy of a dated statement or a timestamped online record; for oral consent, a record of the time and date made at the time of the conversation
- **What** they were told – a master copy of the statement or data capture form containing the consent statement, plus the privacy notice if it was separate, include version numbers and dates. For oral consent, your records should include a copy of the script used.

- **How** they consented – for written consent, a copy of the consent statement or data capture form. If online consent was given, your records should include the data submitted and a timestamp to link it to the data capture form. For oral consent, keep a record of this made at the time of the conversation (you don't need to record the full conversation).
- **If they withdraw** consent and when.

So, for example, keeping a spreadsheet that simply includes the data subjects' names and 'Y' (consent given) against their name, this is not GDPR compliant. If however you kept respondents' signed and dated consent forms this is compliant.

How long consent lasts

The ICO have stated that "*There is no set time limit for consent. How long it lasts will depend on the context. You should review and refresh consent as appropriate*."

Consents should be kept under review and updated if anything changes. This is particularly important for panels, longitudinal MR and for information stored in databases.

What about consents secured before 25 May 2018

If after 25 May 2018 you continue to rely on consent secured before this date i.e. you hold pre-GDPR personal data on file (sometimes called 'legacy data'), you must make sure that this consent is GDPR compliant (this includes records of consent). If it's not, you must secure a new GDPR-compliant consent or find an alternative legal basis to consent or stop the processing. **We advise you to update consents that you will rely on after 25 May 2018 as soon as practical if they aren't GDPR compliant.**

APPENDIX 2

Source: MRS Guidance on Data Protection & Research 2018 published on the MRS website http://www.mrs.org.uk/pdf/MRS%20Data%20Protection%20and%20Research%20Guidance%20Section%201%20_28.04.2018.pdf

4.2.6 Data controllers and consent

Under the GDPR it is a requirement that data controller(s) relying on the consent are named at the time the personal data is obtained. For many research relationships the end-client will be the data controller and the full service agency plus any subcontractors used by the research agency will be the data processor(s). In some cases research suppliers may be joint data controller with the end-client. It is important to note that the end client may still be a data controller even if they do not themselves process any personal data e.g. receive identifiable personal data back from the research supplier. The determining factor is whether the supplier and end-client are jointly "determining the purposes and means" of processing the personal data. The contract between the parties must set out the roles of each party to the contract. However, determination as to who is a data controller or a data processor is a question of fact. Useful ICO Guidance on the difference between data controllers and data processors and the governance implications is available here.

MRS is aware that a requirement to name the end-client upfront at the start of a research exercise such as a survey may have significant consequences in certain research projects such as:

- spontaneous awareness research (assessing whether participants can quote/recall a brand name without prompting)
- reducing methodological rigour including biasing responses where the client's identity is known up front or adversely impacting on trend data where attitudes on behaviour etc are measured over time, as the results will not be comparable.

MRS interprets the requirements in the GDPR on naming the data controller as providing some leeway on the point in time that the controller must be named. It is important that the data controller is named as part of the single process of collecting personal data but this may be more appropriately done at the end rather than at the beginning of a survey. This may be appropriate in those circumstances where researchers, in their documented professional judgement, consider that it will adversely impact the rigour and robustness of the research to name clients at the start of a survey the data controller client must be named at an alternative appropriate point in a data collection exercise subject to the following:-

- it must be made clear to data subjects that the data controller will be named at the end of the data collection exercise
- assurances must be provided to data subjects that any personal data collected will be deleted if at the point that the data controller is revealed they object, wish to withdraw their consent and/or no longer wish to participate.

This approach is most appropriate when no personal data is being shared with the end client but researchers may also consider using it in other circumstances.

It is also important to note that:-

- if client is the source of the personal data then they will also need to be named as part of meeting data subject information requirements

- if client is receiving personal data from the data collection exercise, they will need to be named as a recipient of personal data.

In both cases set out above this information will need to be provided at an appropriate point in the data capture activity, which may be at the end of data collection.

MRS is liaising with the ICO to determine whether this approach is consistent with their interpretation of the provisions in the GDPR and DPA 2018. We will issue additional advice and guidance on this issue on completion of our discussions with the regulator. In light of this members should be aware that advice on this point is subject to change.

Prepared by the BHBIA's Ethics & Compliance Committee May 2018