M3 GLOBAL RESEARCH

Qualitative I Quantitative I Global Studios

# How GDPR Impacts Fieldwork

## 'Grey' Areas and Hot Topics

# Introductions

## Anton Richter

CEO

M3 Global Research

## Neil Phillips

Head of Data

M3 Global Research

## Mo Rice

Senior Vice President

M3 Global Research

## Jana Rueten

Director of Operations (UK)

M3 Global Research



 

# Important Notice:

- The views expressed here are how M3 Global Research sees GDPR impacting on our business. This may be different to how it impacts on other businesses
- This webinar is provided for information and general guidance only. It does not constitute legal advice and is not intended to be relied upon by M3's clients in connection with their own legal compliance. M3 gives no warranties or representations about the content of this webinar and disclaims all liability in respect of it

# 1. End Client Identification

## Background

- The MRS, BHBIA and EphMRA have all provided feedback on discussions with the ICO (Information Commissioner's Office) and subsequently feedback from the EDPB (European Data Protection Board)
- This has been widely taken to mean that end clients must be named for all market research surveys in Europe

# Scenario 1 – Personal Data is collected as part of the survey design

| | Survey Content | Survey Hosting* | Participant Recruitment |
|---|---|---|---|
| Collects Personal Data | ✓ | ✓ | ✓ |
| Data Controllers | MR Agency and possibly end client | Survey Host | Fieldwork Agency |
| Naming Required | MR Agency and possibly end client | Survey Host | Fieldwork Agency |

* Most often this is done by either the MR Agency or the fieldwork company

# Notes on Scenario 1

Aligns with the feedback from the EDPB:

*"We have been informed that the consensus amongst the EDPB group was that, where organisations are jointly determining the purposes and means of processing, they will be considered joint data controllers (in accordance with GDPR Article 26), regardless of whether one controller is only determining the purposes and the other only determining the means.*

*The group was also in agreement that, in a joint controller scenario, where personal data are collected from the data subject, both controllers must be named when the data are obtained (in accordance with the requirements of GDPR Article 13(1)(a)).*

*However this is not formal guidance and further discussions are going to take place".*

*Source: https://www.bhbia.org.uk/latestnews/news/namingclient.aspx*

# Scenario 2 – Personal Data is not collected as part of the survey design†

| | Survey Content | Survey Hosting* | Participant Recruitment |
|---|---|---|---|
| Collects Personal Data | X | ✓ | ✓ |
| Data Controllers | None | Survey Host | Fieldwork Agency |
| Naming Required | None | Survey Host | Fieldwork Agency |

* Most often this is done by either the MR Agency or the fieldwork company
† Be careful that a combination of data points do not together constitute personal data

# Notes on Scenario 2

Recital 26:

*"The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes".*

*Source: https://ico.org.uk/media/about-the-ico/disclosure-log/2014536/irq0680151-disclosure.pdf*

EDPB (at the time named Article 29 Data Protection Working Party)

*"First of all, the mere fact that different subjects cooperate in processing personal data, for example in a chain, does not entail that they are joint controllers in all cases, since an exchange of data between two parties without sharing purposes or means in a common set of operations should be considered only as a transfer of data between separate controllers".*

*Source: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf*

# The Complexities

- It is not always clear when two parties start to share purpose and/or means (and become joint controllers) rather than sharing data without sharing purpose or means (and so being separate controllers)
- The EDBP guidance referenced on the previous slide provides a number of examples and discussion on the topic
- M3 would suggest that you document your decision and how you came to it and note the BHBIA advice

*"The determination of who is a data controller, joint controller, data processor or other party within the research chain is a question of fact rather than contractual stipulation. It is based on a determination of the purposes and means of the processing, and essentially the level of decision-making power exercised".*

*Source: https://www.bhbia.org.uk/latestnews/news/namingclient.aspx*

# In Practice What is M3 Doing?

- While we do not believe it is likely to be necessary, if our client (and potentially their client) determine that they are data controllers or joint data controllers of personal data collected in a survey and wish to identify themselves then we will support this as long as they make it clear that M3 is not providing any of our members' personal data to be associated with the survey responses and remains committed to protecting our members' privacy
- On the other hand, if our clients believe they are not collecting any personal data, and therefore cannot be data controllers of it, then we will support their not being named until and unless further guidance points to the contrary
- In either case it is important to document the decision and the rationale for it

# 2. Qualitative Research Viewing

## Voice as Personal Data

- ESOMAR, MRS, and EFAMRO guidance is that:

*"Sound and video recordings and still images should always be considered as personal data in light of the ease of linking these to a person. Ease of technology in doing this means that there is a higher risk of re-identification of this type of materials".*

*Source: https://www.mrs.org.uk/pdf/EFAMRO_ESOMAR_MRS%20GDPR.pdf*

- The Swedish data protection authority (Datainspektionen) have provided guidance that voice should be considered as personal data
- Others, to our knowledge have not provided specific guidance

## Image as Personal Data

- ESOMAR, MRS, and EFAMRO guidance is that:

- We are unware of any specific guidance but believe it is self evident that an image of someone's face is sufficient to identify them and so should be considered as personal data

# In Person Viewing

- Consent must be obtained for participation and any viewing or recording at the start of the interview
- However, the end client does not need to be named for their in person viewing as data is not transferred to them and they are not processing or controlling any personal data so GDPR does not apply to this activity
- BHBIA Legal and Ethical Guidelines require:

*Live viewing – via one way mirror or sitting-in*

***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.*
- *Before fieldwork starts, you should agree and document the client position on whether you can reveal their identity to respondents if it's requested 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.*

*Source: https://www.bhbia.org.uk/downloads/6285/0/BHBIA_Legal_and_Ethical_Guidelines_July_2018_GDPR_Update_v5FV.pdf.aspx*

# Live Remote Viewing


- Is considered a transfer of data to those viewing so this must be consented before it happens
- All organisations receiving the data must be named as part of the consent process
- BHBIA Legal and Ethical Guidelines require:

*Live viewing – via video relay/streaming, with and without recording*

***Live viewing – via video relay/streaming, with and without recording - Data protection requirements mean you must name the organisation(s) viewing 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.*

*Source: https://www.bhbia.org.uk/downloads/6285/0/BHBIA_Legal_and_Ethical_Guidelines_July_2018_GDPR_Update_v5FV.pdf.aspx*

# Recordings


- Transferring copies of recordings are considered as transfer of data to those receiving them and this must be consented before it happens
- All organisations receiving the data must be named as part of the consent process
- If this would undermine the integrity of the research, consent for transferring to the end client may be done at the end of the interview
- BHBIA Legal and Ethical Guidelines require:

*Delayed viewing – via video-relay (including video streaming and taping)*

*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*

*Source: https://www.bhbia.org.uk/downloads/6285/0/BHBIA_Legal_and_Ethical_Guidelines_July_2018_GDPR_Update_v5FV.pdf.aspx*

# Other Options

- If transcripts are redacted of any personal data then consent to transfer these is not required
- Simultaneous translators can be used to remove the voice of respondents, and thus that aspect of personal data
- Technical means can also distort voices sufficiently to make them unrecognisable
- Pixellation or blurring of faces can be used on video to remove this aspect of personal data

# 3. List Handling

## Assumption

- The end client is the Data Controller of any list they provide
- Fieldwork agency will be a Data Processor of this list
- Data Controller will provide instructions to the Data Processor on what they are to do with the list

## Two scenarios

1. Instruction is to match the list against the fieldwork agencies own panel/database of MR respondents and invite only those that they have a match for (List Match)
2. Instruction includes using the list to directly recruit MR participants (Custom Recruit)

# List Match

- M3 manages a panel of healthcare professionals, patients and other consumers for the purpose of inviting them to participate in MR projects
- As this exists in the absence of any individual client project and M3 are the sole decision makers of what data is collected and how it is processed, we alone are Data Controllers of this data
- A list we are asked by a client to match against our data is a separate activity from the ongoing operation of the panel
  - We process the list on behalf of our clients (according to their instructions)
  - We invite people to participate in surveys according to our own processes
  - Lists do not typically include email addresses and we primarily invite our panel to participate by email
- Our view is therefore that, the list owner does not need to be named as they are not the source of the data which we are using to invite our panel members to participate in a MR project

# Custom Recruit

- If we are using the list to directly approach potential participants the situation is much less clear
- If M3 becomes a Data Controller of the list then according to GDPR we must tell the Data Subject the source of the data – i.e. the client that provided the list
- However, if M3 is acting only as Data Processor then:
  - GDPR requires only that we follow the lawful instructions of the Data Controller
  - ePrivacy Regulations (PECR in the UK) require you to identify yourself if you are conducting marketing although MR is exempt in the UK
- MR guidelines are simpler. EphMRA says:

*"When lists of named individuals are used for sample selection, the source of the list should be revealed to potential MR subjects. The source of the list MUST be revealed to potential MR subject(s) at an appropriate point in the interview, if it is requested. In Germany MR industry guidelines state that MR subjects MUST be told the client company's identity if the client company supplied their name. This can be given at the end of the interview rather than the beginning, but it MUST be given. In Finland, a researcher MUST NOT disclose the identity of the sponsor (unless legally required to do so) to any third party without the consent of the sponsor".*

*Source: https://www.ephmra.org/standards/code-of-conduct/code-of-conduct-online*

# GDPR Principles that have influenced our thinking

- Privacy by Design, and by Default
  - GDPR requires you to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights
  - In essence, this means you have to integrate or ‘bake in’ data protection into your processing activities and business practices, from the design stage right through the life cycle.
- Data Minimisation
  - You must ensure the personal data you are processing is:
    - adequate – sufficient to properly fulfil your stated purpose;
    - relevant – has a rational link to that purpose; and
    - limited to what is necessary – you do not hold more than you need for that purpose

# Consent

- Participants must give their consent for their personal data to be transferred to pharmacovigilance*
- This in turn requires that they be named as part of informed consent
- We believe that this consent can be separate from the survey and collected specific to the AE report

* *Unless they rely upon a different legal basis that we can also depend upon*

# Flow

## If AE identified **during** interview

1. Consent in principle to AE reporting will have been gathered at the start of the interview
2. At end of interview, if an AE is identified, respondent will be informed and any additional information required collected (if possible)
3. Client name will be revealed and consent to pass name/contact information obtained
4. AE Report passed directly to PV

## If AE identified **after** interview

1. Consent in principle to AE reporting will have been gathered at the start of the interview
2. When AE is identified it will reported to PV without contact information
3. If PV request, we will seek consent from the participant (naming the end client) to provide contact information
4. If consent is given, contact information will be passed direct to PV

# 5. Supplier Selection

## Two scenarios

1. Data Controller responsibilities when selecting Data Processors
2. Requirements specific to non-EEA Data Controllers/Processors

# Data Controller Liability

- As a data controller you have broad responsibility in selecting (or allowing) data processors to process data on your behalf
- This starts as requiring you have sufficient guarantees that they will meet GDPR standards
- And extends as far as you believe they have the expert knowledge, reliability and resources to do so

*"…the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation…"*

*Source: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf (Recital 81)*

# Requirements for Overseas Controllers/Processors

- There are specific responsibilities for data controllers and processors outside the EEA
  - They may still need to appoint a DPO and WP29/EDPB recommend* that they should be inside the EEA to allow for sufficient accessibility
  - They need to appoint a representative within the EEA to coordinate with the DPAs
    - This representative can be subject to enforcement proceedings

*3. The representative shall be established in one of those Member States where the data subjects are and whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored.*

*4. The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.*

*Source: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf (Article 27)*



* http://ec.europa.eu/newsroom/document.cfm?doc_id=44100

 

M3 GLOBAL RESEARCH

# Summer Webinar Series

## Patience with Patients: Learnings from building and maintaining patient communities

22 August | 12pm ET / 5pm BST

Presenter: Tom Pugh and Laura Haxton-Wilde

# Q&A

# THANK YOU

M3 GLOBAL RESEARCH