Data Protection Update – Naming the End Client
October 2020

This update aims to explain clearly and simply the circumstances in which an end client needs to be identified to market research participants.

Key Points

There are three independent circumstances in which a commissioning end client would need to be identified to a respondent/data subject.

These are:

The end client is the **source of the personal data** – the source needs to be named to meet data subject information requirements	The end client **receives personal data** (from the data collection exercise) – they will need to be named as a recipient of personal data	The end client **is a data controller** – data controllers relying on consent as their lawful basis for data processing must be named at the time the personal data is obtained from data subjects
E.G. When the end client supplied a list (whether directly or indirectly via a third party) from which a sample will be directly drawn, they have provided the direct and only source of personal data for sample selection	E.G. When the end client views a non-anonymised video stream of fieldwork E.G. When the end client receives AE/PC/ SRS reports that include personal data	When the end client either alone or jointly determines the purpose and means of the data processing

If ONE or more of these three circumstances is the case, then the end client MUST be identified to market research participants/data subjects.

Determination of roles

The determination of who is a data controller, joint controller, data processor or other party within the market research chain is a question of fact rather than contractual stipulation. It is dictated by the role of each party with regard to determining the purposes and means of the processing: basically, roles reflect the level of decision-making power exercised.

The European Data Protection Board's (EDPB) draft *Guidelines 07/2020 on the concepts of controller and processor in the GDPR* refer to 'essential' means and 'non-essential' means, a controller must determine essential means. The guidance also provides some specific (but not exhaustive or definitive) examples:

- Essential means = determining the type of data to be processed, the type of data subjects, length of storage, recipients of personal data;
- Non-essential means = choice of hard and/or software, security measures.

A controller does not have to process personal data directly to be a controller. Even if an organisation does not have access to any personal data it can still be a data controller if it is involved in determining the purpose and means of data processing.

The BHBIA cannot advise members whether they are data controllers or data processors, we can only provide as much relevant guidance as we can, Whatever decision is made by those organisations involved in the data processing must be agreed jointly by the end client and the agency before projects begin and the rationale documented.

Joint sources, recipients or data controllers

There may be circumstances when two (or more) organisations are sourcing personal data, receiving it or acting together as data controllers.

Multiple organisations sourcing personal data

If more than one organisation is the source of an individual's personal data, each organisation must be named.

Example - If a pharmaceutical company supplied a list of names to be matched with a panel held by a fieldwork agency, the pharmaceutical company may be the data controller for their in-house database (from which the list of names they supplied was drawn), the fieldwork agency is the data controller for their panel but the two organisations are likely to be joint sources for the matched list. Whilst both sources have to be identified as the source of the list/personal data, only the fieldwork agency will be in direct contact with the data subjects and so they should be responsible for facilitating data subjects' rights and this should be made clear. Choosing not to name both sources would carry some risk. Of course, this point may be academic if the end client needs to be named because one of the other circumstances applies too.

List matching is a difficult issue on which to provide definitive guidance as the BHBIA and the Market Research Society (MRS) are currently awaiting further advice on this from the ICO. The more conservative interpretation of requirements affecting the example above would suggest that the list resulting from the match is a result of two lists – the original and the panel – and so there are two sources for the matched list (after all it couldn't exist without either one of the two original sources) and so in data protection terms the matched list has two sources – the organisation that supplied the original list and the organisation that

provided the panel. A more pragmatic interpretation might suggest that the producer of the merged list i.e. the panel provider is the sole source but this latter approach may carry some risk.

Multiple organisations receiving personal data

When it is practical to identify the organisations receiving personal data then they must be named. For example, if there are lots of organisations to be named it may not be practical to name them all but this is unlikely to be the case within the work that we do.

Joint data controllers

Organisations jointly determining the purpose and means will be considered joint controllers even if the balance of responsibility when determining purpose and means differs between the two controllers. Determining whether parties are joint or independent controllers depends upon whether they make common or converging decisions i.e. the decision making is inextricably linked.

In this situation both joint controllers must be named irrespective of whether each controller directly processes personal data or not.

When to name the end client

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 to participate at any point
- The justification for this should be documented

HOWEVER the end client receiving personal data MUST be named BEFORE any transfer takes place. So if viewing of non-anonymised film footage is live, the end client must be named before fieldwork takes place.

Not just a UK requirement

It is important to remember that the requirement to name the end client (when they are a data controller, source or recipient of personal data) is not just a UK requirement. This obligation applies wherever the terms of the General Data Protection Regulation (GDPR) or the Data Protection Act (DPA) 2018 apply.

Further updates

When there is further guidance from the European Data Protection Board or the ICO upon interpretation of the definition of data controller we will update members. The BHBIA continues to work with the MRS, the ICO on this issue and is liaising with our European counterparts EFAMRO, EphMRA and ESOMAR too. In view of the ongoing discussions on this issue members should be aware that advice on this point is subject to change so should look out for further guidance.

Appendix

A data controller is defined by the GDPR and DPA 2018 as 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;"*

Article 13 of the GBPR states that:

> *"Information to be provided where personal data are collected from the data subject*
>
> *1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:*
>
> *(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;"*
>
> *(e) the recipients or categories of recipients of the personal data, if any;*

Article 14 of the GBPR states that:

> *"Information to be provided where personal data have not been obtained from the data subject*
>
> *1.Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:*
>
> *(e) the recipients or categories of recipients of the personal data, if any;*
>
> *(f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;*

Further sources

ICO Guide to the GDPR, Key Definitions, Controllers and processors
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/

MRS Data Protection & Research: Guidance Note on Controllers and Processors June 2018
https://www.mrs.org.uk/pdf/MRS_GDPRguidance_controllers_0618%20Final.pdf

Data Protection & Research: Guidance for MRS Members and Company Partners 2018 Part 1 (v0418)
https://www.mrs.org.uk/pdf/MRS%20Data%20Protection%20and%20Research%20Guidance%20Section%201%20_28.04.2018.pdf

European Draft Guidance on Data Controllers and Processors – Update Oct 2020
https://www.bhbia.org.uk/resources/news/edpb-draft-update

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

British Healthcare Business Intelligence Association
Ground Floor, 4 Victoria Square, St. Albans, Herts AL1 3TF
t: 01727 896085 • admin@bhbia.org.uk • www.bhbia.org.uk

A Private Limited Company Registered in England and Wales No: 9244455