Data Protection & Research

Guidance Note on Controllers and Processors

At a glance:
What you need to know and do

Both controllers and processors have direct statutory liability under data protection laws

Your role as a controller or processor is determined on a case by case basis taking into account the facts and evidence of the particular processing situation

Determination of the role that you play in a particular research activity will depend on the level of decision-making power that you exercise over the purposes of the processing (the why) and the means of the processing (the how)

You need to make sure that the allocation of roles is properly documented and reflected in your written contracts

Table of Contents

Section 1: Introduction

This Guidance Note for MRS members and Company Partners explains the distinction between controllers and processors under the General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 (DPA) ("the data protection laws").

At the outset of a research project it may be far from clear who is the controller and who is the processor of any personal data being processed. This Guidance Note is designed to help researchers and clients determine this issue and understand their roles and responsibilities in different types of research activities and projects.

It must be read together with Data Protection & Research: Guidance for MRS Members and Company Partners 2018.

MRS is providing this data protection guidance as general information for research practitioners. 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.

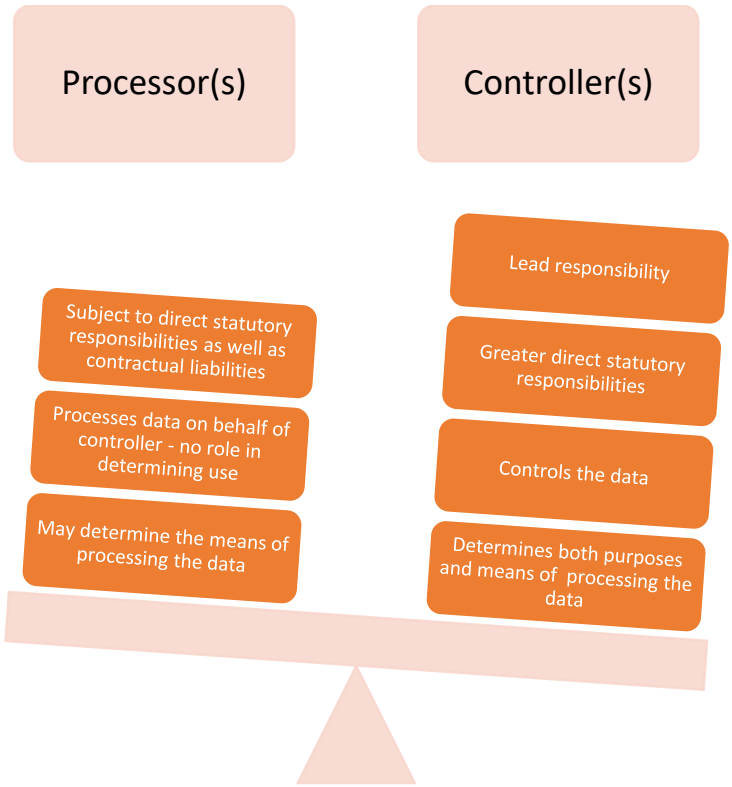
Section 2: Definitions

The data protection laws place specific obligations on all of the parties involved in the research personal data supply chain. This may include the commissioning brand client, a full service agency, panel provider, fieldwork agency, translation supplier, or freelancers such as recruiters and interviewers.

Depending on the role and level of decisions made over a personal data set, the parties may be controllers and/or processors. The responsibilities and liabilities of each party will vary according to the role (see Figure 1). It is important to understand the precise role in order to:

- appropriately meet the data protection principles especially on transparency of processing;
- determine which legal obligations and liabilities within GDPR and DPA are directly applicable to each party;
- enable the parties to reflect the mandatory written contract terms demonstrating compliance with all the data protection law requirements.

Figure 1: Controllers and processors



Controller: *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.*

Joint controllers: Joint determination of the purposes and means of the processing of personal data.[1] Joint controllers does not mean equal controllers. There is some flexibility in allocation of obligations and responsibilities as long as there is full compliance between the parties. Clear allocation of responsibilities is important and this must be documented in contracts.

Processor: *Natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.* A lead processor can also sub-contract to another processor who will be a sub-processor. In a research context an organisation or person is likely to be a data processor where there is processing of personal data solely on the client's behalf such as transcription, processing, analysing, coding, fieldwork and translation activities.

Third party*: 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.* Third parties process personal data on their own behalf. In principle a third party who receives personal data would be a separate new controller.

Recipient: *Natural or legal person, public authority, agency or other body, to which data are disclosed, whether a third party or not.* Recipients are a broader category than third parties as it covers any party to whom personal data are disclosed, including employees of controllers and processors.

Data subject: *Identified or identifiable living individual to whom the personal data that is held relates*.

[1] Concept of joint controller is different from that of "controller in common" previously recognised under UK data protection law as where controllers exercise control over the same data but for different purposes.

Section 3: What is the difference? Responsibilities of controllers and processors

The data protection laws place specific legal obligations on controllers and processors and set out mandatory terms which must be reflected in written contracts. Additional obligations may also be imposed by contract terms.

	Controller	Processor
General obligations	**Controller must be able to:** • Demonstrate compliance with the data protection principles • Implement appropriate technical and organisational measures	**Processor must be able to:** Provide sufficient guarantees to implement appropriate technical and organisational measures
Specific obligations	**Controller must:** • Conduct Data Protection Impact Assessment (DPIA) when required • Provide a point of contact for data subjects • Choose and audit appropriate processors • Enter into suitable contracts with processors • Register and pay applicable data protection fee to the Information Commissioner's Office (ICO) **Joint Controllers must:** • Determine their respective responsibilities by agreement • Communicate the content of the agreement to data subjects	**Processor must:** • Act on written instructions of controller • Co-operate with supervisory authorities such as the Information Commissioner's Office (ICO) • Ensure security of its processing • Keep records of its processing activities • Notify any personal data breaches to controller • Seek written approvals to appoint sub-processor • Seek approval to make data transfers outside of European Economic Area (EEA) • Reflect the same contractual obligations it has with the controller in a contract with any sub-processors Processors are • Liable to the controller for the actions or inactions of any sub-processor • Jointly liable with the controller for certain breaches **Sub- processors must:** • Incorporate same contractual obligations processor has with the controller • Assume same direct responsibilities and liabilities as Processor

Although controllers and processors have specific statutory responsibilities they also have significant common responsibilities as applicable including:

- Appointment of Data Protection Officer (DPO), as required
- Appointment of a representative (if based outside the European Economic Area (EEA)
- Maintaining detailed records (as required)
- Implementing appropriate technical and organisational measures
- Enshrining privacy by design and default
- Recording and documenting the lawful basis for the data processing activities
- Mandatory data breach notification for riskier data breaches
- Ensuring appropriate contracts throughout the supply chain

It should also be noted that:

- Processors act on the instructions of the controller. If the organisation determines the purpose and means of processing (rather than acting only on the instructions of the controller) it will be considered to be a controller with controller liability.
- Processors can be directly liable to controllers under the terms of the contract as well as subject to the enforcement regime of the data protection laws
- Supervisory authorities such as the ICO can take action against both controllers and processors
- Individuals can bring claims for compensation against controllers and processors

For more information see ICO Guide to the General Data Protection Regulation available here.

Section 4: Who are you? Determining your role in a research project

The determination of who is a controller, joint controller, processor or third party is a question of fact rather than contractual stipulation. This means that it is based on an evaluation of who determines the purposes (the why) and the means (the how) of the processing, and essentially the level of decision-making power exercised. It does not rely on which party is making a payment for services.

Parties need to review the facts and evidence for the particular processing activity, reach a decision on the roles, and reflect this in their contract.

The terms of a contract can help to clarify the issue but are not always decisive. Although a contract may specify that a party is only a processor, a supervisory authority such as the ICO in the UK can determine on the basis of a review of the activities that the processor is actually a controller with the respective statutory obligations.

All of these factors can make it quite difficult to determine the precise role of a party within the research data supply-chain and where respective data protection obligations lie. This determination is essentially a reasoned judgement call based on the available facts and evidence for the particular processing situation. In light of this it is important that it is fully considered and properly documented on a case-by-case basis.

4.1 Control and decision-making authority

A client may be a third party, sole controller or joint controller depending on the type of project being undertaken and the level of autonomy and responsibility a client exercises for any personal data being collected. Similarly a research supplier may be a processor, joint controller or sole controller.

The key point in determining the status of each party is the level of control exercised and understanding where decision-making authority is held. Factors identified in the ICO Guidance Note (2014)[2] include understanding which organisation decides:

- "to collect personal data and the legal basis for doing so;
- which items of personal data to collect, i.e. the content of the data;
- the purpose or purposes the data are to be used for;
- which individuals to collect data about;
- whether to disclose the data, and if so, who to;
- whether subject access and other individuals' rights apply i.e. the application of exemptions; and

[2] ICO: Data controllers and data processors: What the difference is and what the governance implications are: https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf

- how long data is retained or whether to make non-routine amendments to the data."

The ICO Guidance details a classic research situation where it considered that the client and the agency were joint controllers as follows:

A bank contracts a market research company to carry out some research. The bank's brief specifies its budget and that it requires a satisfaction survey of its main retail services based on the views of a sample of its customers across the UK. The bank leaves it to the research company to determine sample sizes, interview methods and presentation of results.

The research company is processing personal data on the bank's behalf, but it is also determining the information that is collected (what to ask the bank's customers) and the manner in which the processing (the survey) will be carried out. It has the freedom to decide such matters as which customers to select for interview, what form the interview should take, what information to collect from customers and how to present the results. This means that the market research company is a data controller in its own right in respect of the processing of personal data done to carry out the survey, even though the bank retains overall control of the data in terms of commissioning the research and determining the purpose the data will be used for.

It is important to note that the client and/or research agency can be joint and/or sole controllers over different datasets. In some cases both parties can be sole controllers for different datasets rather than joint controllers. An illustrative scenario is set out in section 5 of this document.

The impact of access to personal data on the determination of the role needs to be clarified. Currently there are divergent legal interpretations on this issue but the grouping of EU regulators, the European Data Protection Board (EDPB), is likely to consider that a commissioning client may still be a controller even if they do not themselves process any personal data e.g. receive identifiable personal data back from the research supplier.

Note: Robust steps must always be taken to protect personal data of data subjects. As research is often based on participant anonymity researchers must obtain precise and enforceable assurances, from clients to ensure that personal data is used in line with data subject expectations and no attempt is made to re-identify data sets where assurances of participant anonymity have been made in a research exercise.

4.2 Research documentation

Research project files must be fully documented, to provide sufficient evidence to support the determinations made on the role of the parties. This will include the following documents:-

- **Client Brief** - Client establishes overall commercial need for insights, analysis or research – the business challenge to be addressed. The level of instruction and degree of specificity for a research approach will depend on the commissioner's needs, their experience and whether they themselves are researchers. For many ad hoc projects a client brief will not set out how personal data should be collected, give a precise means or methodology or specify the individuals to be contacted. The research brief will focus on the challenge to be addressed, the population of interest to be researched, the budget and the timescale. *Note: The more general the client briefing instructions are the more likely it is that the researcher will be a controller.*
- **Supplier Proposal** – Sets out a detailed response to a client brief and addresses specific research objectives; proposed research design, including sample approach, size and structure for primary data collection; proposed research methodology/s; techniques to avoid bias and other methodological rigour; research outputs including whether research results to be shared will be aggregate or individual results; costs; timescales and relevant legal and ethical issues. *Note: The more specific the*

proposal is in determining the purposes and means of the research activity the more likely it is that the researcher will be a controller.

- **Data collection instruments** - Research documents e.g. pre-engagement letters; recruitment screeners; questionnaires, discussion guides, stimulus materials, etc. This participant facing material will reflect the means that will be used for processing the personal data and demonstrate the role played by the researcher in determining the means of processing. *Note: In line with data subject expectations, the more visible the party is to data subjects the more likely it is that the party will be a controller. Taking into account all the other factors such as level of instructions and monitoring of service performance and delivery a less visible research supplier is more likely to be a processor than joint controller.*
- **Contract –** Reflects agreement between the parties based upon a client brief and supplier proposal; commercial terms and conditions (all); mandatory GDPR requirements (if controller/processor); allocation of responsibilities (if joint controller). Contracts are also required with sub-processors.
- **Transparency and risk tools** - Research information statements, privacy policies, legitimate impact assessments, data protection impact assessments may be applicable depending on the research project. These must reflect the role of the parties ensuring privacy policy of the controller is used and participants are clear about how to enforce their rights.

4.3 Decision-making tree

The status of each party is determined by the level of control exercised and where decision-making authority is held. To help you determine whether you are a controller or processor you need to understand who exercises overall control over the "why" and "how" of the data processing.

As a start ask yourself the questions set out below. These are illustrated in the decision-making tree overleaf.

Do you determine the general or specific **purpose (s)** of the data processing (Why)?

- e.g. need for primary research to be undertaken, specific business question to be answered; specific research objectives
- e.g. retention periods for the personal data; application of subject access and individual rights; who has access to the data as set out in the disclosure policy

Do you determine the **means** of processing (How)?

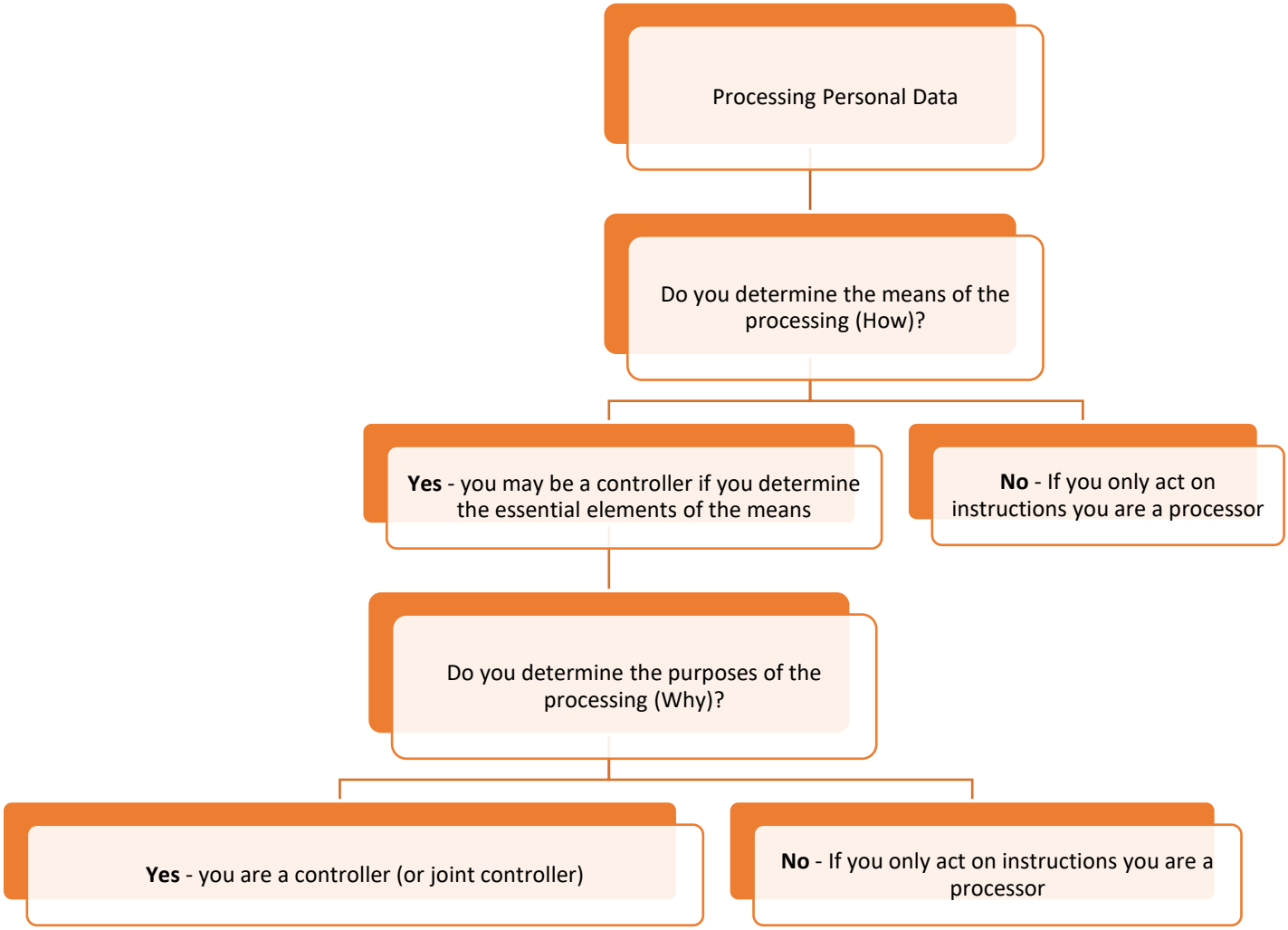
- e.g. the individuals to be targeted as part of the sample frame
- e.g. the appropriate survey platform or software
- e.g. the research methodology

If the answer to both questions is "Yes" then you are likely to be a controller for this processing activity. You may also be a joint controller. Participation between both parties in the "means" or "purposes" of processing the data does not have to be equal for a joint controllership to be established.

If the answer to both questions is "No" then you are a processor for this processing activity.

If you only determine the means, then you may be a joint controller especially if you determine the essential elements of the means such as which data is collected, duration of processing and access to the data.

Figure 2: Controller-Processor Decision Making Tree



Section 5: How does it apply in practice? Case studies in the research sector

The examples below set out some generic examples of the likely controller-processor relationship in some research scenarios. It is important to remember that the determination of roles is fact-specific.

Controller Client – Processor Agency

Client-led research

Client collected personal data from data subjects (e.g. customers) and asks Research Agency to conduct a survey among these data subjects.

Client determines the purpose, as they tell the agency explicitly whom (on an individual basis) to ask. Data may not be used by the research agency for anything else. Client also determines the means of processing of the data by asking the agency to collect and process additional data from the data subjects. Agency process personal data provided by the client under their instructions

Branded client online community

Client commissions research project. Establishes a branded online community and determines terms and conditions of the community. Research Agency contracted to create and manage the community on their platform.

Client determines the purpose as they decide whom (on an individual basis) to recruit and what to ask. Data may not be used by the research agency for any other purpose. Client also determines the means of processing of the data by asking the agency to collect and process the data from the data subjects. Agency process personal data provided by the client under their instructions.

Greater involvement by the research agency in determining the purpose could also create a joint controller relationship.

Joint Controllers - Client and Agency

Agency-led research

Client commissions market research. Agency determines sample sizes, interview methods and presentation of results.

Client determines the general purpose and specific objectives of research exercise but agency decides what questions to ask, how to carry out the processing by survey, which individuals to select for interview, what form the interview should take, what information to collect from customers and how to present the results.

Both parties are involved in determining purposes and means and agency has a high margin of manoeuvre.

If no other organisation is instructed in processing of the data there will not be a data processor in the relationship.

Agency-led research

Research Agency carries out survey on behalf of client. Client describes the target group to be researched and the business questions to be addressed. Research Agency recruits and interviews data subjects (the participants) from the general population i.e. not client-supplied sample. The Client only receives aggregated research reports without personal data.

Research Agency decides whom (on an individual basis) to interview, what to ask (which data). Research Agency obtains the consent from the data subjects (the participants) and might obtain additional data not needed for the report (e.g. home addresses to administrate the allocation of incentives).

Research Agency determines how long the data is kept, who has access and how the data is protected. All of these activities take place without written instructions from the Client.

Controller Client - Processor Agency – Sub Processor Fieldwork Agency

Fieldwork agency

Client commissions research project from research agency with detailed brief based on existing study setting out detailed methodological assumptions. Agency carries out research in line with these instructions. Research agency contracts freelance recruiters or a fieldwork agency to recruit participants based on specific instructions from the client.

Client is a controller as determines both the purposes and the means of processing. Agency is a processor acting on instructions and fieldwork agency is a sub-processor acting on instructions from controller client.

If the contract terms, allow the fieldwork agency to add participant names to a participant database, then the agency will become a separate sole data controller of that dataset. Agency will need to ensure they have a lawful basis for collection of the information. On the other hand if the fieldwork agency breaks the contract terms to use information from the project for an unauthorised purpose such as to build a list for future projects, the organisation will become a separate data controller for this information. It is likely to be in breach of the lawfulness principle and could also commit a criminal offence.

Controller Agency - Third Party Client

Media panel research

Research Agency operates a special panel (e.g. to determine media consumption habits) and has only one customer for the reports. Research Agency is solely responsible for building and maintaining the panel. The Client does not receive any personal data.

Research Agency decides whom (on an individual basis) to interview, what to ask (which data). Research Agency obtains the consent from the data subjects (the participants) and might obtain additional data not needed for the report.

Research Agency determines how long the data is kept, who has access and how the data is protected. All of these activities take place without written instructions from the Client.

Panel research

Panel set up by Research Agency, independent of contracts with customers for the purpose of generating research reports. Regardless of orders, the panel is permanently "maintained" by Research Agency in order to keep it representative. Clients commission Research Agency for research reports without personal data (e.g. market share of toothpaste brand in Lisbon for the target group 49-60 years).

In this case, the Clients do not directly influence the structure and development of the panel and do not receive any information about the panel participants.

The Clients leave it to the Research Agency to determine sample sizes, interview methods and presentation of results. The Research Agency decides whom (on an individual basis) to interview, what to ask (which data). The Research Agency obtains the consent from the data subject (the participants) and obtains a range of personal data for different purposes. Research Agency determines how long the data is kept, who has access and how the data is protected.

Syndicated survey

Financial sector research study across main financial retail markets undertaken by Research Agency. Agency determines areas to be studied and core questions, designs methodology and representative sample. Clients can access results by purchasing syndicated "off the shelf" market reports on main area of interest. Clients have no role to play in determining how long the data is kept for, who has access or how it is being protected.

Controller Processor relationships can vary over different datasets

Research with client sample

Client commissions research project and provides sample from customer database to Research Agency for purposes of contacting potential participants. Sample dataset held within research agency subject to client terms and conditions.

Sample dataset: Controller Client; Processor Agency

Research Agency seeks consent of individuals for survey, conducts survey, analyses responses and provides aggregated data back to the Client.

Research dataset: Controller Agency and/or Controller (or Third Party) Client depending on the levels of control of the parties over the research dataset.

Section 6: Transparency: Obligations on disclosure of client name

6.1 Legal requirements

Transparency is one of the fundamental principles underpinning the data protection laws. In line with this an obligation to name a commissioning client may arise in three main scenarios:-

- *Client is controller or joint controller*[3] - Article 13 of the GDPR requires that the controller(s) are named at the time the personal data is obtained.[4] If a client is a controller they must be named.
- *Client is the source of the personal data*[5] - Article 14 of the GDPR provides that where personal data is not obtained directly from the data subject there is a requirement that the source of the data is disclosed. If a client provides personal data such as sample from a customer database then they must be named as the source of the information.
- *Client is receiving personal data from a research activity*[6] - Article 13 of the GDPR requires that recipients or categories of recipients of data be named. If a client is receiving personal data such as photographs, film, video audio or full transcripts of interviews they must be named as a recipient.

The determination of roles in the research context is presently before the EU grouping of regulators, the EDPB, for review and to ensure consistency of an EU-wide position. In light of this definitive guidance cannot be provided on this issue. In order to meet transparency requirements, those undertaking research will need to decide on the facts of the case and the legal requirements whether there is an obligation to name the client.

Note: If a client is a third party and no personal data is being provided to them they do not need to be named.

6.2 Layered transparency

MRS is aware that a requirement to name the commissioning-client upfront at the start of a research exercise may have significant consequences in certain research projects. It may:

- Reduce robustness and methodological rigour (e.g. biasing responses where the client's identity is known up front; adversely impact on trend data where attitudes on behaviour etc. are measured over time, as results will not be comparable).
- Contravene regulatory controls that seek to ensure there is a clear distinction between direct marketing and other activities (e.g. introducing client name may seem like disguised promotion; routing participants to promotional pages of a client may appear to be a direct marketing activity).

[3] GDPR Article 13 (1)(a)//Article 13 (1)(e)
[4] Recital 42. Also arguable that if no personal information which can identify an individual is passed to client, then client is not relying on consent for the processing, but its legitimate interest.
[5] GDPR Article 14(2);
[6] GDPR Article – consider if relying on consent Recital 42

- Impact on use of methodologies such as spontaneous awareness (e.g. measuring how many participants can recall a brand name or company material without any assistance from interviewer).
- Impact on research that may be 'commercially sensitive' such as when product development or assessing in-licensing opportunities / new assets affects share prices.
- Contribute to information fatigue such as in omnibus surveys, which collect data for a variety of clients, and may require disclosure of the names of multiple clients and their privacy policies.

If a commissioning client is a controller then in accordance with Article 13 of the GDPR they must be named "at the time the personal data is obtained." Different views have been expressed as to whether this requires the client to be named at the beginning of the data collection exercise (such as an interview) or allows some measure of discretion for the client to be named at the end before data collection processing fully starts. Note: *The more broadly that this requirement is interpreted the less likely it will be that the processing is transparent.*

It is important that the controller is named as part of the single process of collecting personal data but in some cases researchers may consider that this more appropriately done in a layered approach i.e. at the end rather than at the beginning of an interview. A layered approach to naming controllers may be considered as 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 data collection. Although it is also clear that this approach will not be feasible for all types of research projects such as longitudinal studies

In all cases if the client is a controller they 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 at recruitment that the 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 controller is revealed they object, wish to withdraw their consent and/or no longer wish to participate and they can of course withdraw their consent at any point.
- Mandatory documentation of approach and rationale for anonymous research or naming client at the end approaches must be included in the research project file.

Data subjects/participants must be provided with access to relevant privacy policies that clearly set out their privacy rights and how they may be exercised. In light of this a layered approach is only likely to be appropriate where researchers and the commissioning client are joint controllers.

Section 7: Accountability: Records and documentation

All researchers must document their processing activities. Controllers and processors have different documentation obligations as controllers need to keep more detailed records, as required by the GDPR and DPA. All parties involved in research must ensure that they properly document processing activities carried out for clients.

The records will vary depending on whether the researcher is acting as a controller or a processor and on the size of the organisation.

Organisations with less than 250 employees record-keeping only need to document processing activities that are not occasional, could result in a risk to the rights and freedoms of individuals or involve special category/criminal convictions data processing. In light of this small research organisations must still fully document all research processing activities as these will not fall within the limited exemption.

Mandatory records of processing

Controllers must keep records of:

- Organisation's name and contact details.
- If applicable, the name and contact details of the data protection officer.
- If applicable, the name and contact details of any joint controllers on a per project basis.
- Purposes of the processing such as market or social research.
- Categories of individuals such as employees, customers, research participants.
- Categories of personal data being processed –different types of information processed about individuals, e.g. contact details, health data, financial data such as bank account details, social network data.
- Categories of recipients of personal data – such as clients.
- If applicable, the name of any third countries (i.e. countries outside of the EU) or international organisations that personal data is transferred to.
- If possible, the retention schedules for the different categories of personal data – how long you will keep the data for as detailed in internal policies or based on industry guidelines and standards.
- If possible, a general description of the technical and organisational security measures e.g. encryption, access controls, staff training.

Processors must keep records of:

- Organisation's name and contact details.
- If applicable, the name and contact details of the data protection officer.
- Name and contact details of each controller on whose behalf you are acting.
- If applicable, the name and contact details of each controller's representative – another organisation that represents the controller if they are based outside the EU, but monitor or offer services to people in the EU.
- Categories of processing carried out on behalf of each controller – the types of things you do with the personal data, e.g. market or opinion research.
- If applicable, the name of any third countries (i.e. countries outside the EU) or international organisations that you transfer personal data to
- If applicable, the name of any third countries or international organisations that personal data is transferred to outside the EU.
- If possible, the retention schedules for the different categories of personal data – how long you will keep the data for as detailed in internal policies or based on industry guidelines and standards.
- If possible, a general description of the technical and organisational security measures e.g. encryption, access controls, staff training.

Documentation on data processing relationship

Controllers and processors must keep records of:

- Evidence base for determination of the nature of the data processing relationship and the roles allocated in contract

Special category/criminal convictions policy document

Controllers of special category data or criminal convictions data, must also develop and maintain an appropriate policy document that explains compliance with the principles and covers:

- the condition for processing in the DPA
- the lawful basis for processing in the GDPR
- the retention and erasure policies

This special category/criminal convictions document must be kept for at least six months after cessation of processing and made available to the ICO on request. Document must be reviewed and updated as necessary.

For a full list of requirements see ICO Guidance on Documentation here

Section 8: Contracts Checklist

Under the data protection laws, a controller must have a written contract with a processor which reflects specific compulsory terms. Joint controllers must also allocate and document their respective responsibilities.

8.1 Checklist: Joint controller agreements

Joint controllers need to consider allocation of responsibilities and reflect these in a written agreement:

- ☑ Determine the applicable privacy policy for the research exercise and address the processing of both data controllers.
- ☑ Allocate responsibilities for which party will deal with subject access requests, data portability requests, deletion requests and at what points of the relationship with the data subject.
- ☑ Ensure breach reporting responsibilities are established
- ☑ Consider apportionment of liability and risks. Researchers need to consider their level of insurance, indemnities and ensure the liability level is reflected in the price of services.
- ☑ Ensure that the mandatory written terms are reflected in contracts with processors
- ☑ Determine the research parameters such as outputs and standard for delivery of anonymised data; re-contact consents; further use of data by any of the controllers
- ☑ Ensure confidentiality assurances to data subjects are reflected in the agreement between research party/s and commissioning client so that clients do not use data in a manner which could compromise assurances given to participants by the agency.

8.2 Checklist: Controller – Processor agreements

Controllers may only appoint data processors which provide sufficient guarantees to implement appropriate technical and organisational measures to ensure processing meets GDPR requirements. Contracts must include the following mandatory terms:

- ☑ Description of
  - Scope, nature and purpose of processing
  - Duration of processing
  - Types of personal data and categories of data subjects
- ☑ Requirement to process data only on the documented instructions of a data controller (including international transfers of personal data)
- ☑ Using only personnel subject to a duty of confidence
- ☑ Keeping personal data secure
- ☑ Using sub-processors only with consent of the data controller (who may provide either specific or general consent)
- ☑ Flowing down obligations in processor contracts with data controllers to any sub-processor (but as data processors you will remain liable to data controllers)
- ☑ Assisting controllers with data subject requests to access, rectify, erase or object to processing of data
- ☑ Assisting controllers with security and data breach obligations and notifying of any data breaches
- ☑ Assisting controllers if they need to carry out a Data Protection Impact Assessment
- ☑ Returning or deleting data at the end of the contract
- ☑ Demonstrating compliance with obligations and submit to data controller audits
- ☑ Informing data controllers, if in a processor's opinion, the data controllers instructions would breach the law

For further information see Draft ICO Guidance on Contracts