# Section 4:
# Data Processing Grounds

**This section discusses the GDPR processing grounds that are appropriate for use in research projects. The grounds discussed are consent of the data subject, the legitimate interests of the data controllers and contractual necessity. Illustrative examples are provided for all the grounds discussed.**

## 4.1 Overview

A legal basis (or processing ground) must be identified before personal data can be processed. There is no hierarchy of processing grounds and data controllers must ensure that the right legal basis is chosen for the data processing activity. Although there are six different legal grounds available, "consent" of data subjects and the "legitimate interests" of the data controller or a third party are particularly relevant to the research sector. In addition to consent and legitimate interest, performance of a contract is also a processing ground for personal data in the context of panel research.[7] Processing grounds give rise to different legal obligations. Data controllers must record which legal ground is being used for the processing activity (with reasons) and detail this in internal data processing records.

In assessing the most appropriate ground to use for data processing researchers must consider the category of data being processed, the nature of the research and the type of data controller. Figures 2, 3 and 4 in this Guidance illustrate how these factors must be taken into account. The grounds that can be used for personal data are set out in Figure 2, the grounds that can be used for special category data are set out in Figure 3 and the grounds that can be used for data processing by public authorities are set out in Figure 5.

In all cases research projects must be conducted transparently and organisations must provide full information to data subjects using a layered and blended approach such as by actively providing some information and making other information easily accessible and using a mix of tools such as infographics, videos, FAQ's etc. to provide access to information.

### 4.1.1. Category of data being processed

The choice of processing ground to be used will depend on whether you are processing personal data, special category data or criminal convictions data.

The UK DPA 2018 requires that where special category data is processed then appropriate policy documentation must be developed that can be made available to the ICO. The documentation must

[7] In particular it is important to note that the use of incentives to encourage participation in research is not a payment for time or participation and are not part of a contractual relationship with data subjects. Different arrangements may apply for panel providers.

- explain how the controller complies with the data protection principles,
- set out retention and erasure policies, and
- be kept for at least 6 months after cessation of processing.

If you are processing special category data you must have a lawful basis under Article 6 of the GDPR in addition to meeting a special condition under Article 9 of the GDPR but these grounds do not have to be linked.

#### 4.1.2. Nature of research being carried out

The choice of processing ground will also be determined by the type of research (such as whether it is possible to get informed consent) or if the research is for scientific, historical or statistical research purposes or in the public interest.

Under the DPA 2018, scientific or statistical research by private sector, public sector, third sector or academic bodies that is in the public interest can use the research exemption as a processing ground for special category or criminal convictions data. The regime for scientific or statistical research carried out in the public interest are further detailed in section 5 of this Guidance and in separate guidance (MRS/SRA Public Interest Research Guidance forthcoming May 2018).

#### 4.1.3. Type of data controller

Public authorities cannot generally rely on legitimate interests as a processing ground for research activities. In this case the most relevant legal basis is likely to be processing "in the public interest". However, the standards for use of legitimate interests and public interest will be similar, requiring a balancing of the interests of the data controller and the data subject.

**For further information see:**

- MRS/EFAMRO/ESOMAR Guidance Note Different Legal Basis under the GDPR
  https://www.mrs.org.uk/pdf/EFAMRO_ESOMAR_MRS%20GDPR.pdf
- ICO Guide to the GDPR
  https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

## Figure 2: Personal data processing grounds for research (Article 6 GDPR; Section 7 DPA 2018)

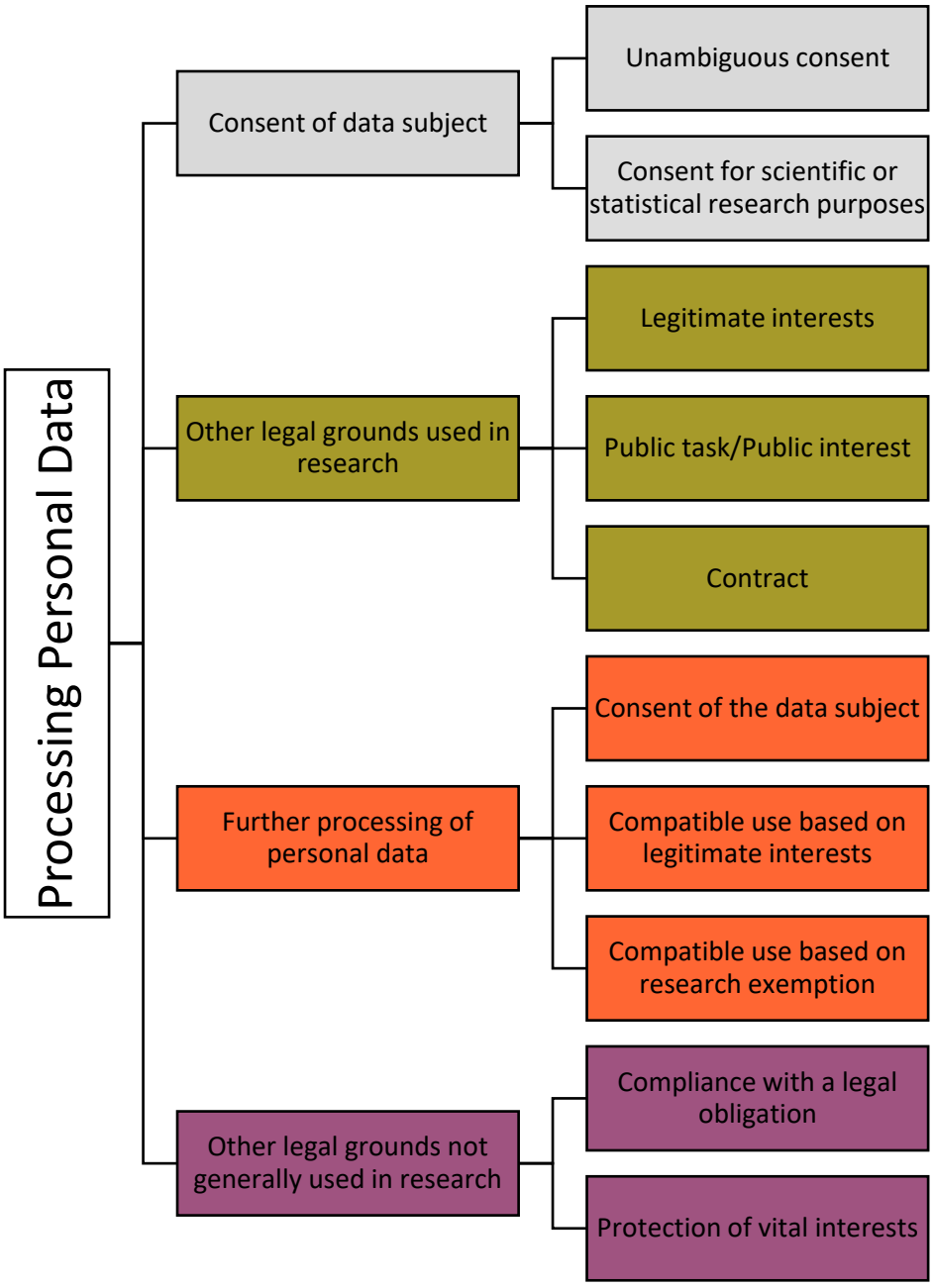
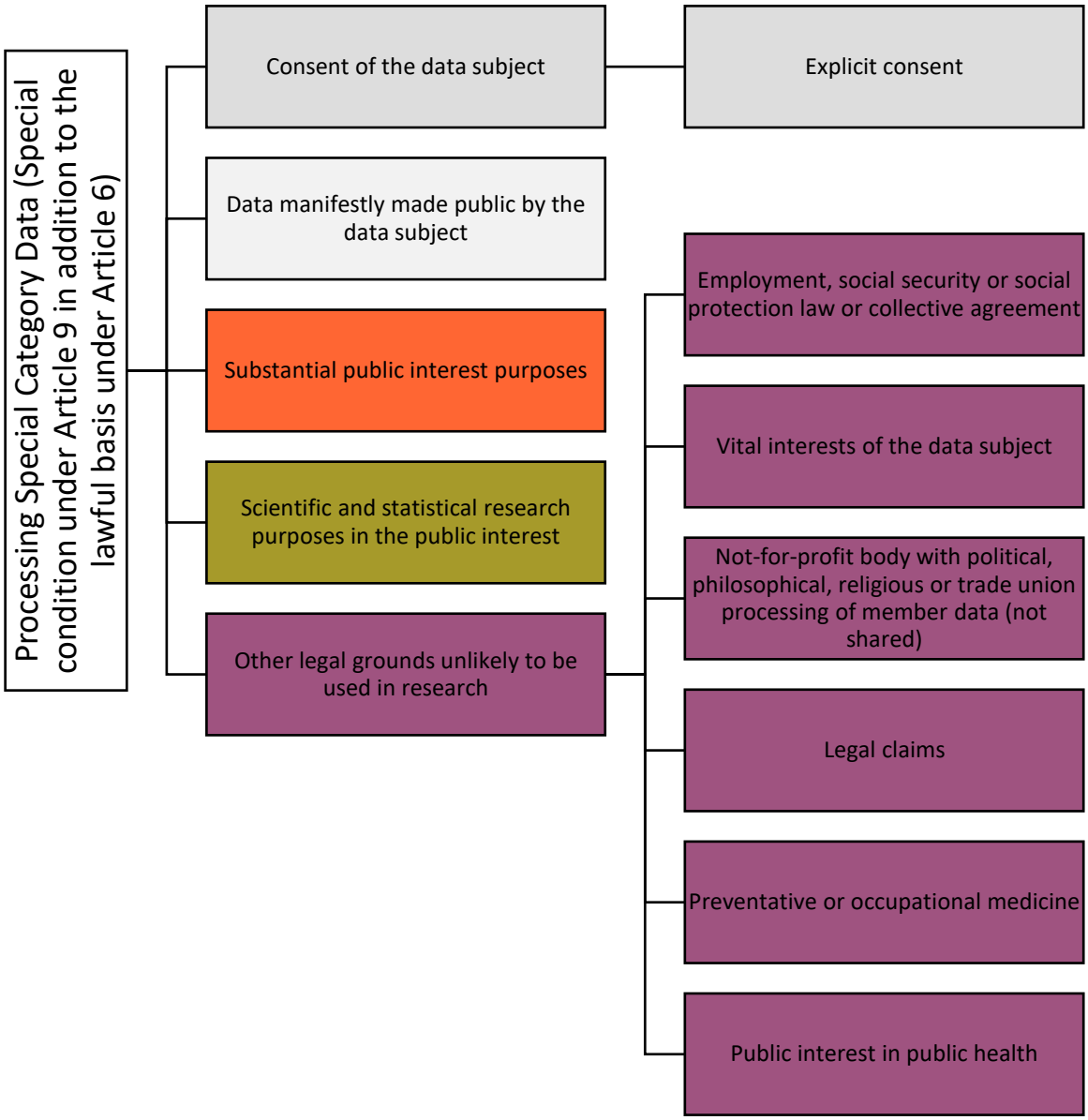


Figure 3: Special category data processing grounds for research (Article 9 GDPR; Section 9 & Sched. 1 DPA 2018)



## 4.2 Consent

Consent can be used for all types of data collection and researchers can also use a modified consent regime where undertaking scientific research in the public interest (as discussed in Section 5 of this Guidance). Obtaining consent of data subjects in adherence with the GDPR is more challenging than previously as the requirements are more detailed and robust than the requirements in the DPA 1998.

Consent is essentially about individual choice and control, and although it will often be the right lawful basis for carrying out research, researchers must be certain that consent is the most appropriate ground for any research project.

### 4.2.1 General conditions for consent

Consent may be given in writing, electronically or orally. If, as a researcher, you use consent for data processing you must ensure that the individual's consent is:

- freely-given
- specific to the research purpose(s) which must be highlighted to data subjects
- informed
- unambiguous indication given by clear affirmative statement or action and clearly distinguished from other terms and conditions. Silence, pre-ticked boxes or inactivity cannot be used to give consent.

Researchers must allow data subjects to give separate consent for all personal data processing activities. Separate consents must always be sought to conduct research, re-contact data subjects for specified future research purposes and/or to use data subject video or visual images such as recordings and photos.

Written, electronic and oral consent are all valid but consent must always be verifiable in order to demonstrate that consent was legitimately obtained. For consent obtained orally this could include noting when and how consent was obtained against individual data subject records e.g. Jane Doe consented by phone on 25th May 2018 at 10:30 a.m. Note made by A. Researcher at 10:35 a.m. on 25th May 2018 together with a record of the script used in the conversation.

### 4.2.2 Conditions for explicit consent

Reliance on explicit consent is required for:

- collection of special category data or criminal offences or convictions data.
- automated decision-making and/or profiling with legal or significant effects.
- international data transfers to countries outside the European Economic Area (EEA) that are not deemed adequate by the EU.[8]

Explicit consent must be given by a very clear and specific statement of consent. EU guidance specifies that explicit consent can be obtained by a signed written statement; by the individual sending an email, uploading a scanned document carrying the signature or by using an electronic signature.

Researchers collecting special category data or criminal convictions data as a core part of a research project must ensure that they obtain and record a specific statement such as "Name/Signature/Data agree to take part in this research study which will collect data about my physical health and religious beliefs

[8] Countries within the EEA includes all EU countries and non-EU countries Iceland, Liechtenstein and Norway. The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US (limited to the Privacy Shield framework) as providing adequate protection. Adequacy talks are ongoing with Japan and South Korea.

and attitudes."

Special category data and/or criminal convictions data may also be collected as part of a demographic classification exercise for research projects or as a requirement for equal opportunities monitoring. If answering these questions are optional (such as with a prefer not to say option) then explicit consent can be sought at the point that the classification questions are posed. If the special category data is being sought as part of equal opportunities monitoring, then these is a specific substantial public interest legal ground under DPA 2018 that can also be used.

If there is automated processing of information and/or profiling of data subject with significant legal effects, then data subjects must be given information about the processing explaining what information will be used, why it will be used and what the effects might be. Also, if explicit consent is being used to authorise data transfers to third countries (in the absence of an adequacy decision and appropriate safeguards), then data subjects must be informed about the possible risks of these transfers.

#### 4.2.3. Consent of children

Researchers must note that under the MRS Code of Conduct, children are data subjects who are under the age of 16. The Code requires that researchers seek the consent of a responsible adult prior to seeking the consent of a child (data subject under the age of 16) to participate in a research exercise. This rule applies to all channels of research e.g. online; digital; face-to-face; telephone or postal.

This Code requirement is a higher requirement than the DPA 2018. Under the DPA 2018 the following rules apply:

- parental consent must be sought in relation to processing of personal data for online services, for children under the age of 13
- children over the age of 13 can give their own consent in relation to processing of personal data for online services
- competence of the child must be assessed where relying on consent and/or performance of a contract as the legal ground.

In all cases research exercises with children must be carefully reviewed to ensure children are properly protected when you are collecting and processing their personal data (particularly as they may be less aware of the risks). Additionally, privacy information notices must be tailored and written in a manner that is easily understood by the target age group of children or young people.

Researchers must always adhere to the MRS definition of a child as under 16, not to the DPA 2018 definition of a data subject under the age of 13.

#### 4.2.4. Recording consent

Robust records must be kept of all consents obtained demonstrating who consented, when they consented, what they were told, how they consented, whether they have withdrawn consent and if so, when. This should include:

- who consented (name of individual, or other identifier (e.g. online user name, session ID);
- when they consented (copy of dated document; online record with timestamp; note of time and date which was made at time of conversation);
- what they were told (master copy of document or data capture form containing consent statement used at time; record of scripts used in getting oral consent);

- how they consented (relevant document or data capture form; for online consent data submitted as well as timestamp to link to relevant version of data capture form; note of oral conversation but not necessarily a full record of conversation; audio recording of confirmation of the consent);
- whether they have withdrawn consent and, if so, when.

#### 4.2.5 Minimum information requirements for consent

Data subjects must be provided with all relevant information to make choices about the collection and retention of their data. Different techniques and formats can be used to get consent for data collection but, in all cases, the consent must be specific and informed with transparent disclosure of all required information. Pre-ticked boxes or opt-outs are not allowed.

There is a minimum level of information that must be provided as part of the process of getting consent. As applicable this includes:

- data controller(s) identity and contact details –details of the data controllers relying on the consent (this may be both the research supplier/s and the client where they act as joint controllers) preferably allowing for different channels of communication (e.g. phone, email, postal address)
- purpose of each processing activity that consent is being sought for (such as for research, re-contact for future research);
- type of personal data to be collected and used;
- existence of the right to withdraw consent;
- information about the use of the personal data for decisions based solely on automated processing, including profiling;
- possible risks of data transfers to third countries outside the EEA in the absence of an adequacy decision or appropriate safeguards

This information must be provided prior to getting consent and must be included on a consent form or in the script being read to data subjects to seek verbal consent for their participation.

#### 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.

### 4.2.7. Data subject rights

In addition to the information that is provided to research data subjects as part of the process of obtaining informed consent, data subjects also have the right to the following specified information when consent is used as the basis for data processing:

- contact details of data protection officer(s) (if applicable)
- legal basis for processing;
- details of any international data transfer outside of the EEA;
- retention period for data or criteria for retention;
- existence of any automated decision making and logic, significance and consequences; and
- details of all other rights including right to object, right to data portability, right to withdraw consent; right to lodge complaints with supervisory authorities.

Data subjects also have other rights:

- to withdraw consent at any time (must be as easy to take away as to give);
- to port data (if automated information collection);

- to erasure of data made public (and data controller will need to inform other controllers who may be processing);
- to restrict processing;
- to access data;
- to rectify data held;
- to object to the processing; and
- to not be subject to decision based on automated processing (including profiling) which produces legal effects or significantly affects them.

All of the rights must be promoted at each contact point. If data subjects withdraw their consent for use of their data, the data controller must ensure that any personal data is deleted from any study or database in which the data subject is still identifiable.

If there are joint data controllers the privacy information notice that will be applicable to the research must be agreed between the controllers so that it can easily be made available to research data subjects. It must be completely clear to the data subject which data controller can be approached in order for them to exercise their rights under the GDPR.

In determining whether consent or another ground is the right ground. Organisations should note that consent can be withdrawn (and processing must stop immediately) however if an individual objects on the basis of legitimate interests an organisation has an opportunity to defend the decision. Additionally, an individual's right to erasure is automatic if processing is based on consent but it is not automatic for processing based on legitimate interests. In the later case of legitimate interest processing an individual has a right to object and the right to erasure would apply if the processing is not justified and if the data is no longer required for processing purposes.

All of this information must be set out in clear and plain language in a privacy information notice.

#### 4.2.8 Consent for recordings and in digital environments

Consent for audio, video and other visual images

In seeking consent for the use of visual images, particularly video clips, researchers must ensure that:

- data subjects have been fully briefed and informed about their use particularly where the video clips and/or images will be shared on social media platforms.
- clients have agreed to use the visual images data only in line with the consents provided by data subjects.

Consent for electronic communications

- Collection of personal data in electronic communication services e.g. online services, will be impacted by the reforms to the e-Privacy Directive and Privacy Electronic and Communications Regulations in the proposed e-Privacy Regulation. This may lead to consent being used as the legal ground in additional situations, such as third party analytics used to measure and assess number of visitors to a website. Final version of the e-Privacy Regulation is expected in 2019.

**Consent in practice**

Consent is suitable for a range research approaches such as:

- Panel research
- Qualitative and quantitative research based on free found recruitment or recruitment of data subjects face to face, in store, in street recruitment or random digit dialling
- Customer satisfaction research
- Online or digital surveys

# Consent Example No.1

## Qualitative study

A fieldwork agency is commissioned by a research agency to recruit members of the public to participate in focus groups assessing a brand's dental products. The research agency designs the screener and recruitment script. It also carries out the interviews (moderating the focus groups), analyses the data and writes the report for the client. At recruitment the data subject is provided with a consent form that allows them to sign and give a written declaration of their consent. The form details the name of the client and the research agency. It also sets out the purpose(s) of the research for which consent is being sought as to "gather views of the public on the packaging design of dental products". It allows the individual to consent separately to video recording and to re-contact for follow-up research on the same products by the client within the next 6 months. The consent form also sets out that the individual has a right to withdraw consent at any time. A full privacy information notice is provided at the time that the data subject signs the consent form.

In this case the research agency and the client will be joint data controllers, with the fieldwork agency acting as a data processor. This approach would be sufficient to get informed consent for the project. If the data subjects are being recruited on the basis of health characteristics e.g. regularly bleeding gums and/or the research will cover impact of the use of the products on their health, then it will be important to highlight that the research is health related (i.e. is special category data) in the consent statement to be signed by the data subject.

Additionally, to meet other data protection requirements, the agreement between the joint data controllers must also set out whose privacy information notice will be used and who the data subject should contact to exercise any of their data protection rights. The agreement between the research agency and the fieldwork agency should ensure that any personal data is securely transferred between them. Appropriate organisational and technical measures must be in place which will depend on the risk attached to the data and to the transfer.

# Consent Example No. 2

## Observation Research

Researcher displays a prominent notice in a supermarket informing data subjects that photographs and/or recordings are being made and used for research purposes. Members of the public having been so informed, decide to go to the area in which this is being done. Consent can be inferred by affirmative action in entering the building.

# Consent Example No. 3

## Telephone Survey

Research call centre carrying out a Random Dialled (RDD) survey asks data subjects for specific permission at the outset of a call for the survey research. Records of consent are kept in a spreadsheet with "consent provided" ticked against the data subject's name.

The oral consent is acceptable however it will need to be fully documented. Agencies need to keep details such as date, time, individual making call, script used. It may be best practice to have consent in a durable medium such as a recording that can be evidence of consent. Recording would start after consent obtained and confirm that interview proceeding as consent was given. Details of how data subjects can access the privacy information notice will also need to be provided such as by providing website link; offering to email data subject or providing a phone number they can contact to hear additional information.

# Consent Example No. 4

## Quantitative Tracking Study

Data subjects are required to click on a box to enter a survey. A privacy information notice is provided. A statement with a tick box signifying the individual's agreement is necessary for the collection of any special category data. Best practice requires that specific explicit consent is sought upfront for surveys where the main subject matter of the survey is on special category data. However, consent for collection of special category data such as for categorisation purposes can be sought at the point in the online survey where these demographic questions are asked of the data subjects.

**For further information see:**

- MRS GDPR In Brief (No.5): Informed Consent (Member Content)
- MRS GDPR In Brief (No.6): Informed Consent Checklist (Member Content)
- ICO Guide to the GDPR (consent) https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

## 4.3 Legitimate Interest

Legitimate interest (LI) is a flexible processing ground that can be used as a basis for collecting and processing personal data in research projects. LI is likely to be most appropriate where the data is being used in ways that individuals would reasonably expect and the processing is unlikely to have a significant impact on their privacy.

In using LI organisations are processing data based on legitimate interests pursued by the data controller (such as a client) or on the legitimate interests of a third party. The type of interests that can qualify as legitimate interests are broad and include processing for all types of research purposes, as well as commercial activities such as direct marketing. In determining whether LI can be used, organisations will need to ensure that their interests are not overridden by the fundamental rights and freedoms of the data subject. Particular care must be taken in considering the rights of children.

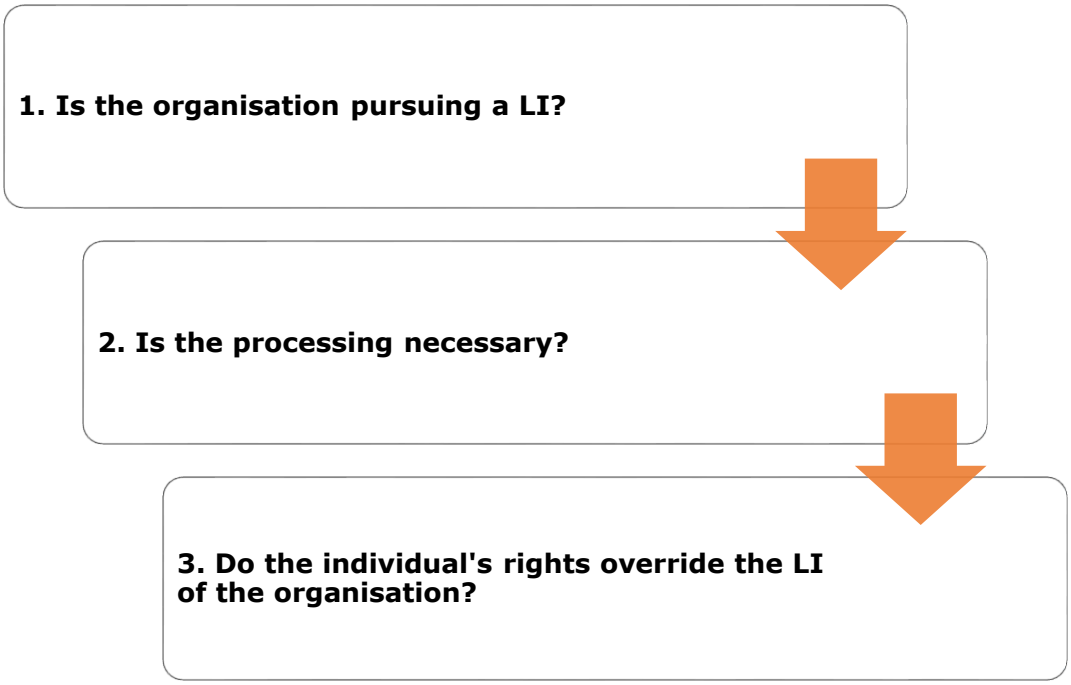
A range of interests will qualify as legitimate interests. It is important to be clear as to whose legitimate interests are being considered. The legitimate interests may be those of the researcher acting as a data controller, such as where a research agency recalls data subjects for quality control purposes, (even where they have not consented to a recall for research). Theymay also be the legitimate interests of the client as data controller, such as when a researcher contacts customers on a client database to ask them to participate in research to understand customer satisfaction levels with the client's products and/or service. It may also be a researcher's interest as a third party to access a database. The GDPR does not allow public authorities to use LI as a processing ground. However, under the DPA 2018, public sector bodies are likely to be able to rely on legitimate interest grounds when carrying out non-public tasks.

#### 4.3.1 Legitimate Interest Assessment - Approach to using LI as a processing ground

Researchers using this processing ground will need to follow and document a three stage approach. The process of considering, weighing interests and making a justified decision must be applied and documented in a Legitimate Interests Assessment (LIA):

1. Purpose – Is a legitimate interest being pursued?
2. Necessity – Is the processing necessary?
3. Balancing – Do the individual's interests override the legitimate interest of the organisation?

## Figure 4: The Legitimate Interest (LI) Test




**Purpose** Is there, and if so, what is the legitimate interest being pursued?

The GDPR sets out a non-exhaustive list of potential legitimate interests, including prevention of fraud. Regulatory guidance in this area also makes it clear that the nature of the interest can vary and encompasses trivial as well as compelling interests.

In order to identify the legitimate interest ICO recommends that organisations consider:

- Why do you want to process the data – what are you trying to achieve?
- Who benefits from the processing? In what way?
- Are there any wider public benefits to the processing?
- How important are those benefits?
- What would the impact be if you couldn't go ahead?
- Would your use of the data be unethical or unlawful in any way?

**Necessity** Is the processing necessary?

In order to use LI the processing must be necessary to pursue the interest. The proposed processing of the data does not have to be the only way to pursue the interest, but it should be a reasonable way of proceeding. This requires the organisations to consider the targeting and proportionality of the processing.

Organisations need to consider whether there are less intrusive or more privacy enhancing means of processing the personal data for the organisation's legitimate interests. The type of data being processed and context in which it was collected will all impact on the determination as to how intrusive the processing is.

In order to apply the necessity test the ICO recommends that organisations consider:

- Does this processing actually help to further that interest?
- Is it a reasonable way to go about it?
- Is there another less intrusive way to achieve the same result?

**Balancing** Do the individual's rights override the LI of the organisation?

The legitimate interests of the organisation must be balanced with the interests of individual. In order to balance interests by considering the impact of the processing and whether this overrides the interest the ICO recommends that organisations consider:

- What is the nature of your relationship with the individual?
- Is any of the data particularly sensitive or private?
- Would people expect you to use their data in this way?
- Are you happy to explain it to them?
- Are some people likely to object or find it intrusive?
- What is the possible impact on the individual?
- How big an impact might it have on them?
- Are you processing children's data?
- Are any of the data subjects vulnerable in any other way?
- Can you adopt any safeguards to minimise the impact?
- Can you offer an opt-out?

It is important to look at the

- impact on data subjects such as the possible level of harm
- way the data is being processed
- reasonable expectations of data subjects
- safeguards that could be put in place.

Balancing the data controller's rights against the rights of the individual in a research context means that you should structure and carry out the research in the least intrusive and most privacy-enhancing way.

Organisations need to keep a written record of reasons why it is felt the balancing test was met. This important in order to meet the GDPR accountability principle.

Conducting market, opinion and social research activities is likely to fall within the legitimate interests of the data controller, but as discussed, written documentation justifying this must be developed and kept by the data controller.

Detailed guidance on conducting a legitimate interests assessment in a research context is set out in Section 7 of the Guidance (forthcoming July 2018).

### 4.3.2. Limitations of LI

Although LI is a flexible processing ground it places an onus on the organisation attempting to use it to ensure that individual's rights and interests are fully considered and protected.

LI must not be used as a processing ground:

- by public authorities (unless the processing is outside their scope of tasks as a public authority)
- for automated decisions based on profiling activities
- for processing of special category data

LI should be used with caution as a processing ground for children's personal data and extra care taken to ensure interests of children are fully protected. It is also important that researchers ensure that in line with the MRS Code of Conduct personal data of children under 16 is only collected after seeking consent of a responsible adult to approach the child to get their consent.

### 4.3.3. Transparency and LI

In order to rely on LI the organisation must set out its legitimate interests in privacy information notice. Researchers relying on LI to carry out research on customers databases for example would need to ensure that a proper explanation of LI for research has been included in the client's privacy notice setting out the basis for using LI.

> *Example of LI statement*
>
> *Name of organisation/We process personal data/information for certain legitimate business purpose which include undertaking research to:-*
>
> - *better understand how people interact with our websites*
> - *better understand how people choose and/or use our products and services*
> - *determine the effectiveness of our promotional campaigns and advertising*

Data subjects have similar rights to situations where processing is based on consent, but they also have the right to object to processing for legitimate interests without providing specific reasons. Also, data subjects do not have a right to port or move their data (as this only applies where data gathered on the basis of consent or contract) and the right to erasure is not automatic as it is with processing based on consent.

#### Legitimate interests in practice

Legitimate interest is suitable for a range of approaches including:

- Customer satisfaction, awareness and usage surveys (on customer databases)
- Quantitative or qualitative research using customer databases
- Research using existing data sets or third party data (i.e. data not directly provided by individual or where no contractual relationship) such as social media analytics
- Secondary processing such as data analytics on loyalty card data or on mixed brand datasets customer behaviours, preferences and movements. If unable to contact all participants then need to use the flexibility in the information obligations where contacting all participants for scientific research would involve a disproportionate effort.

# Legitimate Interest Example No. 1

## Client supplied list

Client company transfers customer data list to a research company for the supplier to develop a sample/target group for satisfaction research exercise. List includes customers who have objected to being contacted for marketing. The list can be used on the legal basis of legitimate interests of the client once the LIA has been undertaken and the client's interest is compatible, the client's privacy note details their legitimate interests as including research and no special category data is being collected as part of this exercise. Researcher must check that the opt-out from marketing contacts is not drafted so widely as to cover opt outs from market research.

Decision making process for this must be documented.

# Legitimate Interest Example No. 2

## Audience measurement

Radio station commissions a research agency specialising in audience measurement to provide data on audience/ visitors. The analytics are used to assess number of visitors, page views etc. for tailoring/optimisation of future marketing campaigns. Aggregate reports are provided grouped under headings such as age brackets, gender, geographical location, socio-economic bands). Aggregate reports are produced for the client. Agency pseudonymises data and disposes of data after original purpose fulfilled. Contract between the client and research agency prohibit attempts to re-identify data. Reports are not used for individual targeting or advertising to research data subjects.

This may be an allowable legitimate interest under GDPR. It is an area where the legal requirements may become more stringent following the proposed ePrivacy Regulation and reform of Privacy and Electronic Communication Regulations (PECR). Balancing test will need to be carried out and documented detailing the business interests and individual's right.

**For further information see:**

- ICO Guide to the GDPR (Legitimate Interests) https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/
- ICO Legitimate Interests Guidance (forthcoming)
- DPN Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation (July 2017) https://www.dpnetwork.org.uk/dpn-legitimate-interests-guidance/
- IAF Legitimate Interests and Integrated Risk and Benefits Assessment (September 2017) http://informationaccountability.org/wp-content/uploads/Legitimate-Interests-and-Integrated-Risk-and-Benefits-Assessment.pdf

## 4.4 Contract

Contract can be used as a legal basis for processing personal data. Researchers can rely on this if they need to process someone's personal data in order to fulfil their contractual obligations to them. This ground will be of limited use but may be applicable to administration and management of research panels.

Panel providers can use contracts as the legal basis for recruitment to research panels for processing that is necessary for the contract between them and the research panellist. Data subjects are likely to join a panel on the basis of the terms and conditions of the research panel provider. These terms and conditions together with the privacy policies and notices will provide information to data subjects about the collection, processing, use and storage of aggregated and personal data, plus any specifics relating to the providers activities.

If contractual necessity is being used as the legal ground this must be documented, with reasons clearly set out in the organisation's records. Data subjects must also be informed that this is the basis for processing their personal data. This ground is likely to be applicable only to the arrangements for adding a panellist to the panel database. Collection of personal data for individual research projects e.g., surveys will need to be conducted on the basis of consent and in particular contract cannot be used a ground for processing special category data. This will generally be processed on the basis of explicit consent of the data subject.

A contact does not have to be in writing in order to be legally binding however researchers using this ground must ensure that the terms and conditions with panellists are recorded in writing so that they have a full documented record of what has been agreed between the parties.

For processing based on contractual necessity, data subject rights are applicable including their right to port data but

- no right to object to processing
- no right not to be subject to a decision based solely on automated processing.

### Contract in practice

Contract is not generally a suitable basis for processing research data but can be used in the following circumstances:

- General terms and conditions for administration of the panel
- Incentives payment and management

## 4.5 Further processing (Secondary use of personal data)

In line with the purpose limitation principle in the GDPR, personal data must be collected for well-defined purposes and not further processed for additional purposes. Exceptions to this are where the secondary use of the data is:

- based on consent
- compatible with original data collection purposes
- for scientific or statistical research purposes or
- based on an EU or Member State law

Secondary use of data occurs when data is used for a purpose different from the purpose for which the data was initially collected. A processing ground is still required for this secondary use of data and the GDPR sets out a compatibility test for re-use of data not based on consent.[9]

### 4.5.1 Further processing based on consent

Personal data can be further processed if consent for the specific purpose has been obtained from the individual at the outset of data collection. If the data controller processes data based on consent and wishes to process the data for a new purpose, then the controller needs to seek a new consent. There is no scope for processing for further "compatible" purposes to inherit the original consent as a basis for processing. In light of this, researchers must define as well as possible any further, secondary purposes when collecting consent at the outset of the research project. If the research project is scientific research in the public interest it may be possible to provide additional information with greater granularity as the project progresses but this should not be used as a default option. Additional information on using the research regime is set out in section 5 of this Guidance.

### 4.5.2 Further processing based on legitimate interests

Legitimate interests of the data controller can also be used to further process data as long as this processing is for a compatible purpose.

Key points in determining compatibility are (this is not a limited list):

- Link between the purpose the personal data was initially collected for and the purpose it is proposed the data be used for
- Context and relationship between the data subject and the data controller
- Nature of the personal data
- Possible consequences of processing the personal data
- Safeguards used in processing such as encryption or pseudonymisation of data

Researchers will generally be able to justify the further use personal data (initially collected for another non-research purpose) using the legitimate interests of the data controllers/clients as the processing ground. In these circumstances, a research purpose is likely to be compatible with the original data collection and processing purpose.

[9] GDPR Article 6(4)

If personal data is being used for scientific and/or statistical research it is deemed compatible under the GDPR.

Researchers must first check to see whether a research project can be carried out with de-identified or anonymised data. It is also important to recognise that special category data can only be re-used where explicit consent is provided. Remember that special category data cannot be processed on the basis of legitimate interests.

### Further processing in practice

Further processing can be used for a range of research approaches such as:

- Re-using data for research
- Purchased secondary data
- Sharing purchased data
- Open access secondary data

## Further processing Example No. 1
## Data analytics

Retailer using loyalty card data gathered for research. Reasonable expectation that retailer would use this data to gain a better understanding of customers and the market. Acceptable and likely compatible further processing using legitimate interests as the legal processing ground.

## Further processing Example No. 2
## Combining datasets

Retailer looking across datasets and combining this with other publicly accessible data (such as information legally obtained (i.e. in accordance with the terms and conditions) from social media platforms Facebook, Twitter, Pinterest, LinkedIn) to instruct interaction with particular data subjects (e.g. targeted advertising). It is unlikely this would meet the compatibility requirements for further processing based on legitimate interest. It would also require analysis of other rules such as direct marketing/profiling and requirement to ensure compliance with data minimisation principle and conduct a DPIA.

**For further information see:**

- *ICO Guide to the GDPR*
  **https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/**

## 4.6 Summary of processing grounds in research

| Processing Ground | Category of Data | Types of Research Activity | Public-facing documentation |
|---|---|---|---|
| **Contract** | Personal | No research activity<br>Use for general terms and conditions for administration of the panel and incentives management for panellists | Contract terms and conditions<br>Privacy policy |
| **Consent** | Personal<br>Special Category<br>Criminal Convictions | Panel research<br>Qualitative and quantitative research (free found recruitment or recruitment of data subjects face to face, in store, in street recruitment or random digit dialling)<br>Customer satisfaction research<br>Online or digital surveys<br>Further processing based on new consent | Consent statement<br>Privacy Policy<br>Special category policy document (as applicable) |
| **Legitimate Interests** | Personal | Customer satisfaction research (on existing customer databases)<br>Quantitative or qualitative research using customer databases<br>Research using existing datasets or third party data (i.e. data not directly provided by individual or where no contractual relationship) such as social media analytics<br>Data analytics on loyalty card data<br>Compatible further processing of data collected using another processing ground | Summary of Legitimate Interest Assessment (make available)<br>Privacy Policy setting out legitimate interests |
| **Research exemption** | Special Category<br>Criminal Convictions | Published social research projects<br>Public health research<br>Longitudinal studies<br>Further processing for scientific research | Special category policy documentation<br>Summary of research exemption public interest assessment (make available) |