BHBIA
ETHICS & COMPLIANCE

# Data Protection requirements

## Lawful Bases for Processing of Personal Data

## Introduction

In order to process personal data market researchers and data analysts must have a 'lawful basis' for doing so. This guidance explains some of the lawful bases that are available under the General Data Protection Regulation (UK GDPR) and the UK Data Protection Act (DPA) 2018.

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.

*The Information Commissioner's Office (ICO) guidance on lawful bases - https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/*

## A lawful basis for data processing

Within the UK GDPR/DPA 2018 there are six lawful bases for processing personal data. Of these, two are likely to be used regularly for commercial market research (MR) and data analytics (DA):

- Consent
- Legitimate interest

Generally speaking, MR often relies on consent for its data processing, whereas DA often relies on legitimate interest. Deciding which lawful basis to use depends on the circumstances. In some contexts, the lawful basis of 'contract' could be used (e.g. for panel companies or where the activity veers towards a 'consulting' type of activity instead of MR); the assessment of whether 'consent' or 'contract' may be more appropriate is up to the companies involved in the activity and this guidance will not focus on it. Additionally, a fourth basis of 'public task' may be used (where data processing is carried out in the public interest or on public authority, with a clear basis in law), however this is unusual in commercial healthcare business intelligence and as such this guidance will not focus on it either.

It is worth taking time to consider the data needs and business requirements as failure to properly address issues of informed consent or another identified lawful basis may restrict the opportunities for initial collection and subsequent use of data.

# Consent

Consent under UK GDPR/DPA 2018 refers to:

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

Consent is the freely given, specific, and informed and unambiguous agreement by a person (i.e. the 'data subject' or 'participant') to take part in the market research (MR) and for the processing of their personal data. It involves a participant voluntarily confirming their willingness to take part in a particular project, after having been informed of all aspects of the project that are relevant to their decision to participate.

## Consent must be:

- Given by a **clear affirmative action**, e.g.
  - Signing a written statement
  - Answering yes to an oral request
  - Ticking/checking an opt-in box online or on paper
  - Clicking an opt-in button or link online
  - Selecting from (equally prominent) yes or no options
  - Choosing technical settings or preference dashboard settings
  - Responding with a positive answer to an email requesting consent
  - Volunteering optional information for a specific purpose, e.g. dropping a business card into a box to enter a prize draw.

- **Freely given** – consent wouldn't be considered freely given if there is a clear imbalance of power between the person or organisation requesting consent and the data subject. If for example healthcare professionals are involved in the recruitment of patients or healthcare consumers for an MR exercise, great care must be taken that the patient/healthcare consumer does not feel undue pressure to participate simply because they were asked by a doctor.

- **Specific** (to a single purpose) – different personal data processing activities should have separate consents, e.g. consent to store individuals' personal data on a database, consent to video record their participation in a group discussion for analysis, consent to share such a recording with the commissioning client. Consent must specifically cover all purposes the personal data may be used for. Thinking ahead and anticipating potential uses of the data will allow you to secure all the consents you could need.

- **Clear** – unambiguous, concise and easy to understand, using simple and clear language.
- **Prominent and obvious**, not 'bundled up' with other terms and conditions

- **Verifiable** – you must be able to demonstrate that someone has consented, whether that is through signature or recording a date/time that the consent has been given

- **Informed**
  - **If personal data are to be obtained directly from an individual**, e.g. via an MR screening interview, the information above must be delivered when that personal data is collected, i.e. at recruitment.
  - **If the personal data are <u>not</u> obtained directly from the individual**, e.g. via digital listening or desk research, the information above must be delivered:
    - If the data are to be used to communicate with an individual, then at the latest at first communication with the data subject
    - If the data are to be shared/disclosed with another organisation, at the latest when the personal data are first disclosed.

    The information must be delivered within a reasonable timeframe (one month at the most) of the personal data being obtained. This provision is subject to certain exemptions cited in Article 14 of the UK GDPR.

It is possible to 'layer' the information so the consent is collected when it is relevant with the aim not to overwhelm the data subject. Consent to participate, recording and/or observation could for instance be collected during the initial recruitment interaction with the data subject (alongside informing them about their right to withdraw), whereas more detailed information about how the data subject is able to exercise their right access that personal data and withdraw consent for its processing could be provided in a separate document such as a privacy policy available as a separate document (e.g. via email) or online.

BHBIA
ETHICS & COMPLIANCE

To be informed, consent must include:

- ✓ **Name and contact details of the data controller(s)** and where applicable the data controller's representative and the data protection officer
- ✓ The **type of company commissioning the MR** (if they are not deemed a data controller or recipient of personal data)
- ✓ The **recipients or categories of recipients of the personal data** e.g. the name of the commissioning client if they are to be given access to non-anonymised recordings to respondents participating in MR
- ✓ **Lawful basis for processing**
- ✓ **Purposes** of the processing – how the personal data is intended to be used
- ✓ **Types of processing activity** – what you will do with the personal data
- ✓ **Where processing is based** and **details of any data transfer to countries without an existing 'adequacy decision'** (generally countries outside the European Union and with whom the UK has no adequacy agreement)
- ✓ **How long the data will be stored** for or, if that's not possible, the criteria used to decide the retention timeframe
- ✓ **Right to withdraw consent** at any point and other data subject rights - to have their personal data rectified or erased, to access or move their data, to restrict or object to data processing in future and to complain to the data protection authority (the Information Commissioner's Office (ICO) in the UK) - some of the detail could be put in to the privacy notice. It must be as easy to withdraw consent as it was to give it, so it should be an easily accessible single step. It is good practice to tell individuals how to withdraw their consent.
- ✓ **Existence of any automated decision making** and its consequences (if applicable)
- ✓ **Contact details of data protection officer** where applicable

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

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

Researchers and analysts need to provide all the information above to secure consent under UK GDPR/DPA 2018 requirements and they must also provide the information detailed within the BHBIA's Guidelines (e.g. the methodology, duration of fieldwork, reimbursement offered etc.). For further details see section E4.2 and E6.1 of the BHBIA's Legal & Ethical Guidelines, available on the BHBIA website - https://www.bhbia.org.uk/guidelines-and-legislation/legal-and-ethical-guidelines

BHBIA
ETHICS & COMPLIANCE

## For more detail about:

- **The different consents that might be required** during the course of a primary market research project and at what stage these consents must be secured; and
- The requirements for **naming the data controller(s)**

please see the BHBIA's guide ***'Consents for Market Research - What is required and when'***, available on the BHBIA website.

## Explicit consent

Explicit consent is not clearly defined within the UK GDPR/DPA 2018. It can be considered to be a slightly higher standard of consent and may be necessary for:

- Processing special category (sensitive) personal data such as health data. (While there are other lawful bases available to legitimise processing special category persona data, they are unlikely to apply to MR and data analytics.)
- Automated decision-making including profiling; please note: profiling is not the same as creating a segmentation.
- Overseas transfers to countries without existing adequacy decisions or other appropriate safeguards in place.

Consent that is inferred from someone's actions cannot be explicit consent, however obvious it might be that they consent. Explicit consent must be confirmed in a clear and specifically worded statement (oral or written). The ICO advise that if you need explicit consent, you should take extra care with the wording. The following example may help to explain the distinction:

- ✘ *For your information, when you participate, we will collect health data about you* – this is not explicit consent as the respondent does not indicate their active agreement with the proposed processing, and even the fact that they may actively provide you with the information may not meet the threshold for 'explicit' consent;
- ✓ *I consent to you collecting the health data I may provide to you for the purpose of market research* – this is explicit consent

## Children and Consent for MR

If a child under 16 years of age is intended to be approached for their consent to participate in MR, BHBIA and Market Research Society (MRS) guidelines currently require you to secure parental or the legal guardian's verifiable permission first. Additionally, if the MR is going to take place online, the requirements of the Children's Code (Age Appropriate Design Code) will apply.

If you rely on children's consent, you must have age-verification measures in place and make 'reasonable efforts' to verify parental responsibility.

## Recording consent

Respondents' consent or refusal must be recorded; consent may be given:

- Verbally during telephone recruitment/fieldwork
- By clicking on an acceptance box if the work is carried out online or via a mobile device
- In writing if recruitment/fieldwork is face to face.

To satisfy the requirements of the UK GDPR/DPA 2018, your records should include:

- **Who** consented – the individual's name or other identifier (e.g. online username, session ID)
- **When** they consented – a copy of a dated statement or a timestamped online record; for oral consent, a record of the time and date made at the time of the conversation
- **What** they were told – a master copy of the statement or data capture form containing the consent statement, plus the privacy notice if it was separate, include version numbers and dates. For oral consent, your records should include a copy of the script used.
- **How** they consented – for written consent, a copy of the consent statement or data capture form. If online consent was given, your records should include the data submitted and a timestamp to link it to the data capture form. For oral consent, keep a record of this made at the time of the conversation (you don't need to record the full conversation).
- **If they withdraw** consent and when.

For example, keeping a spreadsheet that simply includes the data subjects' names and 'Y' (for 'Yes, consent given") against their name would not be compliant with data protection law. If however you kept respondents' signed and dated consent forms this would be compliant.

### How long consent lasts

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

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

**Withdrawing Consent**

Individuals have the right to withdraw their consent at any time they want to. This right must be respected and their personal data and market research input must be withdrawn from the records and destroyed. It must be as easy to withdraw consent as it was to give it.

## Legitimate interests

### What using legitimate interests as a lawful basis means

Market researchers and data analysts may be able to process personal data on the basis that it is necessary to the 'legitimate interests' of the data controller (e.g. the commissioning client company) or a third party (e.g. a fieldwork agency acting on behalf the client). Legitimate interests can potentially also be used as the lawful basis for the secondary use of personal data, for instance exports from CRM systems for use within MR or Data Analytics.

Using legitimate interests as a lawful basis to process personal data requires you to be able to justify why the processing is necessary to pursue the data controller's commercial or business objectives. This need must be balanced against the rights of the individual and what is fair and reasonable for them. There are certain situations

where legitimate interests may be a preferred lawful basis, e.g. when processing data on customers and securing their consent is impractical.

Individuals have the same rights as with consent, with the exception that they have the right to object to the processing, and that they do not have the right to data portability. In addition, the right to be forgotten does not necessarily apply under legitimate interests if the data controller can justify an overriding and continued necessity to process the personal data.

## Determining whether it's appropriate to use legitimate interests

Whether it is appropriate to use legitimate interests or not will depend upon the outcomes of a risk assessment usually called 'Legitimate Interest Assessment'. Its component tests should be carried out in this order:

1. **Purpose test**
    - Is there a legitimate interest (specific purpose) for the proposed processing of personal data?
    - Whose legitimate interest is it (commissioning client, MR agency, fieldwork agency)?
2. **Necessity test**
    - Is the processing necessary to achieve the stated purpose and is the planned methodology of processing proportionate to that purpose?
3. **Balancing test**
    - Is the legitimate interest overridden by the data subject's interests, rights or freedoms, e.g. due to unjustified adverse impact on the individual?
    - Could the data subject reasonably expect the processing to take place? For instance being approached for healthcare MR could be within the reasonable expectations of healthcare professionals.
    - What safeguards can be put in place (e.g. data minimisation, anonymisation, encryption)?

The decision-making process will need to be documented, e.g. via the use of a Legitimate Interest Assessment template as provided by the ICO. If you do not, you may not be able to meet your obligations under the 'accountability' principle without it. The ICO provides further guidance on legitimate interests here: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/ A Legitimate Interest Assessment template can be found here: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/

## Privacy information for data subjects when using legitimate interests

You will need to have a **privacy notice stating the purpose/legitimate interest**. You are still required to provide clear and comprehensive information about how you will use the personal data when personal data is processed under the controller's legitimate interest:

- If the personal data you are processing under this lawful basis was not obtained directly from the data subjects, then you will need to consider your options for complying with Article 14, meaning that privacy information will need to be made available:

  - If the data are to be used to communicate with an individual, then at the latest at first communication with the data subject
  - If the data are to be shared/disclosed with another organisation, at the latest when the personal data are first disclosed.

  The information must be delivered within a reasonable timeframe (one month at the most) of the personal data being obtained. This provision is subject to certain exemptions cited in Article 14 of the UK GDPR.
- If the personal data you are processing under this lawful basis was obtained directly from the data subject for one purpose but any secondary processing is for another (new) purpose and which your risk assessment (such as a Legitimate Interest Assessment) does not demonstrate is compatible with the original purpose for which the data was collected/processed, then you are likely to have to obtain consent from data subjects for the new purpose.

Legitimate interests may be an appropriate lawful basis for processing an individual's personal data when for example:

- A commissioning client company provides a list of customer names (originally collected for marketing purposes and held on a customer database) to an agency to draw a sample from for the purposes of customer satisfaction MR or awareness and usage work
- Third party data (e.g. collected from social media) is used for a secondary MR purpose (such as the MR analysis of contributors' comments), assuming that MR is a compatible purpose with how and why the personal data was first provided.

### When it's not appropriate to use legitimate interests

It is important to note that legitimate interests cannot be used as a lawful basis for:

- Processing special category (sensitive data) e.g. health data
- MR carried out by public authorities
- Automated decisions based on profiling activities.

## The 'research' exemption

Article 89 of the UK GDPR provides for certain "safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes".

This allows (amongst other things and subject to certain conditions):

- Processing of personal data for scientific research with broad (i.e. not specific) consent
- Secondary use of personal data for research for a compatible purpose.

While in some contexts you may be able to demonstrate that the research exemption applies (e.g. for public health research), the Information Commissioner's Office notes that it "is unlikely to apply to the processing of personal data for commercial research purposes such as market research or customer satisfaction surveys, unless you can demonstrate that this research uses rigorous scientific methods and furthers a general public interest."[1]

[1] ICO, "A guide to the data protection exemptions": https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/a-guide-to-the-data-protection-exemptions/, 24 February 2025

BHBIA
ETHICS & COMPLIANCE

## Next steps

- Identify the lawful basis for your data processing and document it
- Review and if necessary revise your consent statements and privacy notices for forthcoming projects
- Review and if necessary update your consents and privacy notices for legacy data
- Make sure your record keeping policies and processes are appropriate and keep comprehensive records

## Additional sources

**Information Commissioner's Office** guide to lawful basis
https://cy.ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/

**Information Commissioner's Office** guidance on consent
https://cy.ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/

**Information Commissioner's Office** guidance on legitimate interests
https://cy.ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/

**Information Commissioner's Office** on the research provisions
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/the-research-provisions/

**EFAMRO & ESOMAR**, General Data Protection Regulation (GDPR) Guidance Note for the Research Sector: Appropriate use of different legal bases under the GDPR, June 2017
https://www.esomar.org/uploads/public/government-affairs/position-papers/EFAMRO-ESOMAR_GDPR-Guidance-Note_Legal-Choice.pdf

**MRS – Market Research Society** - Guidance on the General Data Protection Regulation (GDPR) and data protection for social research
Guidance on the General Data Protection Regulation (GDPR) and data protection for social research | Market Research Society

**Updated by the BHBIA's Ethics & Compliance Committee August 2025**

**British Healthcare Business Intelligence Association**
**St James House, Vicar Lane, Sheffield, S1 2EX**
**t: 01727 896085 • admin@bhbia.org.uk • www.bhbia.org.uk**
**A Private Limited Company Registered in England and Wales No: 9244455**