BHBIA

BHBIA Ethics & Compliance

Preparing for the General Data Protection Regulation

GDPR – Legal Grounds for Data Processing

Introduction

In order to process personal data market researchers and data analysts must have a 'legal basis' for doing so. This guidance explains the some of the legal bases that will be available to us under GDPR.

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 ICO will be publishing finalised guidance on consent and the BHBIA may need to update its guidance as more information becomes available.

A lawful basis for data processing

Within the GDPR there are six lawful bases for processing personal data but only two are likely to be used regularly for commercial market research (MR) and data analytics (DA):

- Consent
- Legitimate interests

Generally speaking consent is used more frequently within MR and legitimate interests in DA. Deciding which legal basis to use depends on the circumstances. A third basis 'public interest' may be used but as this would be unusual in commercial healthcare business intelligence we are not focusing on this in these guidelines.

Consent

The GDPR definition of consent is similar to but a little more detailed than the Data Protection Directive definition. Consent under GDPR 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 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 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, so that if for example doctors are involved in the recruitment of patients for a MR exercise, great care must be taken that the patient does not feel undue pressure to participate simply because they were asked by a doctor.

- **Specific** (to a single purpose), different 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 this with the commissioning client. If securing separate consents would be unduly disruptive or confusing it may not be necessary but as a minimum, consent must specifically cover all purposes. 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.

  It is possible to 'layer' the information i.e. provide it in chunks in a step wise fashion e.g. tell respondents they have a right to withdraw in the consent statement, tell them how this can be done in the privacy policy and provide the privacy policy as a separate document or online.

- **Prominent and obvious**, not 'bundled up' with other terms and conditions

- **Verifiable** – you must be able to demonstrate that someone has consented

- **Informed**
  - **If personal data are to be obtained directly from an individual** e.g. via a MR interview, the information overleaf must be delivered when it's obtained i.e. at recruitment.
  - **If the personal data are <u>not</u> obtained directly from the individual** e.g. via digital listening or from a customer database, the information overleaf must be delivered:
    - When the first communication takes place If the data are to be used to communicate with an individual
    - If the data are to be shared/disclosed before this happens.

To be informed it 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 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
- ✓ **Legal basis for processing**
- ✓ **Purposes** of the processing – why you want the data
- ✓ **Types of processing activity** – what you will do with the data
- ✓ **Where processing is based** and **details of any data transfer to countries without adequate data protection** (generally countries outside the EU)
- ✓ **How long the data will be stored** or if that's not possible, the criteria used to decide this
- ✓ **Right to withdraw consent** at any point and other 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 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.
- ✓ **Existence of any automated decision making** and its consequences
- ✓ **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 GDPR 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 - www.bhbia.org.uk

For more detail upon:

- **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
- **Naming Data Controller requirements**

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

Explicit consent

Explicit consent is not clearly defined within the GDPR but it is basically a slightly higher standard of consent and is necessary for:

- Processing special category (sensitive) personal data such as health or financial data. There are other ways to legitimise processing special category data but these are unlikely to apply to MR and data analytics.
- Automated decision making including profiling (profiling under the GDPR refers to the use of an individual's personal characteristics of behaviour (e.g. for the purposes of direct marketing). Profiling is not the same as segmentation.
- Overseas transfers to countries without adequate safeguards.

Explicit consent must be confirmed in a clear and specifically worded statement (oral or written), so signing a statement would be explicit consent but an affirmative action alone such as responding to an email requesting consent would not be explicit consent. The ICO advise that if you need explicit consent, you take extra care with the wording. The following example helps to explain the distinction:

✘ *We will provide* [the client] *with film footage of the group discussion to help them understand the market research better* – this is not explicit consent

✓ *I consent to you providing* [the client] *with film footage of the group discussion to help them understand the market research better* – this is explicit consent

Consenting children into MR

BHBIA and MRS guidelines currently require you to secure parental consent to approach a child to ask for their consent to participate in MR if the child is under 16. The GDPR requires parental consent for children under 16 to use online services provided at the user's request ("information society services"). The 2018 UK Data Protection Act is likely to lower this age to 13. If you rely on children's consent, you must have age-verification measures in place, and make 'reasonable efforts' to verify parental responsibility.

Keeping records of consent

The GDPR requires you to keep records of the consents secured. Your records should include:

- **Who** consented – the individual's name or other identifier (e.g. online user name, 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.

So, for example, keeping a spreadsheet that simply includes the data subjects' names and 'Y' (consent given) against their name, this is not GDPR compliant. If however you kept respondents' signed and dated consent forms this is 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.

What about consents secured before 25 May 2018

If after 25 May 2018 you continue to rely on consent secured before this date i.e. you hold pre-GDPR personal data on file (sometimes called 'legacy data'), you must make sure that this consent is GDPR compliant (this includes records of consent). If it's not, you must secure a new GDPR-compliant consent or find an alternative legal basis to consent or stop the processing. **We advise you to update consents that you will rely on after 25 May 2018 as soon as practical if they aren't GDPR compliant.**

Legitimate interests

What legitimate interests mean

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 interest can potentially also be used as the legal basis for the secondary use of personal data for instance, within CRM systems.

Using legitimate interests as a legal basis to process personal data requires that you must 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 interest may be a preferred legal basis e.g. when processing data on customers and securing their consent is impractical.

Individuals have the same rights as with consent *except* they do not have the right to data portability if the legal basis is legitimate interests *and* the individual has the right to object. In addition, the right to be forgotten does not necessarily apply (where legitimate interest is used as a basis for processing) if the data controller can justify an overriding and continued necessity to process the data.

Whether it's appropriate to use legitimate interests

Whether it is appropriate to use legitimate interests or not will depend upon:

- **Whether the processing is necessary and proportionate**, the controller must make the case and document the decision making process determining the necessity e.g. because individuals can't be given a clear, genuine choice or where consent is inappropriate.

- **Balancing the subject's rights, freedoms and interests** against the controller's interests – there should be no unjustified adverse impact on the individual.
- **Whether the purpose of the data processing could be reasonably expected** by the data subject – at present it is expected that MR would be within the reasonable expectations of customers/contributors. Similarly in a business to business scenario (e.g. a pharmaceutical company engaging with the NHS), the processing of customer information is likely to be considered a reasonable expectation of the customer.
- **Having a privacy notice stating the purpose/legitimate interest**. Even if you are not requesting consent, you still need to provide clear and comprehensive information about how you will use the personal data, stating where data is being processed under the controller's legitimate interest.

Legitimate grounds may be an appropriate legal 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. provided via social media) is used for a secondary MR purpose (such as the MR analysis of contributors' comments), assuming that MR is a compatible purpose

When it's not appropriate to use legitimate interests

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

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

Necessary steps to using legitimate interests

1. Determine the legitimate interest

- Whose is it – the commissioning client company, MR of fieldwork agency or recruiter?
- What is the legitimate interest?

2. Determine whether the processing is necessary and proportionate

- Is there a more privacy enhancing legal basis (e.g. consent) that could be used?
- Is the processing required to uphold a relevant and appropriate relationship, or for direct marketing for instance.
- If the purpose is secondary research, is this compatible with the original purpose and within the reasonable expectations of the data subject?

3. Balance the interests of the data controller with those of the data subject

- What is the impact on the data subject?
- What safeguards can be put in place (e.g. data minimisation, anonymization, encryption)?

4. *Document the decision making process (sometimes referred to as the balancing test)*

- Record all the factors taken into account to arrive at the decision, this must be done to meet accountability requirements.

The Data Protection Network provide a 'Legitimate Interests Assessment template' within their *Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation*, July 2017, available at https://www.dpnetwork.org.uk/dpn-legitimate-interests-guidance/

The 'research' exemption

Article 89 of the GDPR states that:

> "*Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide exemptions to data subject rights*".

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.

However it is not clear yet whether MR or DA carried out for a commercial purpose could qualify as 'research' under the exemption and what specific provisions may apply. Public health research will be included within the research exemption.

Once confirmed, it is generally expected that the terms and conditions of the research exemption will be applied consistently across the EU including the UK.

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:

ICO's GDPR Consent Guidance CONSULTATION, March 2017
https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

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

Data Protection Network, Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation, Data Protection Network, July 2017
https://www.dpnetwork.org.uk/dpn-legitimate-interests-guidance/

Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, wp259, adopted 28 November 2017
http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

Prepared by the BHBIA's Ethics & Compliance Committee February 2018

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

A Private Limited Company Registered in England and Wales