bhbia.org.uk

FAQ - Privacy & Data Protection

This resource is based on based on queries that members have sent to our ethics advisor or raised at meetings, grouped under a series of headings.

Please note: this does not provide comprehensive coverage of everything you need to know about GDPR. Please also consult the **Privacy & Data Protection** section, for the latest guides, which include links to other online information.

The FAQs are grouped into the following areas:

If you cannot find the answer to your question in the resources provided, you can submit a new query to our Ethics Advisor. Please use the guidelines and legislation Online Enquiries Form. (This service is only available to full BHBIA members only and you will need to log in).

Responses given are not legal advice and if a legal opinion is required this should be sought separately. The information given in the response is for information purposes only. Whilst every reasonable effort is made to ensure the information is accurate, no responsibility for its accuracy or for any consequences of relying on it is assumed by the authors.

Naming the end client

We (the pharma end client), don't tend to receive any personal data such as the name of the respondent – does the advice about naming the client still count in these circumstances?

Unfortunately, yes it does. According to the ICO's advice and the view of the European Data Protection Board (EDPB) you can still be a data controller (responsible for determining both the purpose and means of the data processing) without ever receiving/processing any personal data.

For more details see the BHBIA's *Consents for Market Research – what is required and when guide* and our various updates on naming end clients as data controllers - you can find links to these here

As an end client I am concerned about commercial sensitivity if we have to be named – and also confusion for the respondent about why

we are being named if the research is not promotional. Is there any way around this or do we need to stop doing research in the UK?

If you decide that you are a data controller then you do need to be named (though this could be at the end of the interview).

We have further feedback on the 'data controller issue' following a meeting of the European Data Protection Board's (EDPB) key provisions sub-group, which was attended by all the major Member State Data Protection Authorities (DPAs) including the ICO. The EDPB is the EU body in charge of the application of the GDPR.

We have been informed that the consensus amongst the EDPB group was that, where organisations are jointly determining the purposes and means of processing, they will be considered joint data controllers (in accordance with GDPR Article 26), regardless of whether one controller is only determining the purposes and the other only determining the means. The group was also in agreement that, in a joint controller scenario, where personal data are collected from the data subject, both controllers must be named when the data is obtained (in accordance with the requirements of GDPR Article 13(1)(a)). **This thinking is in line with the ICO's advice and makes it clear this is not a UK only issue.**

Please see our various updates on naming the end client as data controller - you'll find the most recent in the Privacy & Data Protection section.

How do we resolve concerns about disguised promotion – especially when researching pipeline drugs – if we are required to name the client? Should we explain to the respondent that we are doing it because it's a GDPR requirement, and it is not intended to be promotional in any way?

Yes, this is exactly what we should be doing.

Please also note that the ABPI Code says:
5.5 Material relating to medicines and their uses, whether promotional or not, and information relating to human health or diseases which is sponsored by a pharmaceutical company, or in which a pharmaceutical company has any other involvement, must clearly indicate the role of the company. The only exception to this is market research material if it is such that the name of the company involved is not required to be stated; then the material must state that it is commissioned by a pharmaceutical company.

Ref: https://www.pmcpa.org.uk/the-code/

Obviously the GDPR requirement to name the client as data controller overrides the ABPI guidance that naming the client is optional, but the important point to note is that naming the client is not in conflict with the ABPI Code, and does not, in itself, imply any disguised promotion.

If you have determined that the client is a third party, and they are not receiving any personal data, do you still have to name the client if the respondent asks?

No, as long as it's clear that the client is not a data controller, then they would not need to be named in this case unless there is a contrary legal obligation e.g. they provided the contact list.

It would be important to document the rationale for determining that the client is not a data controller – i.e. the justification for deciding that they are not determining both the purpose and means of the data processing.

Please see our various updates on naming the end client as data controller - you'll find the most recent in the Privacy & Data Protection section.

If our MR client tells us (the fieldwork agency) that they believe their end client is not a data controller, can we go ahead without naming them? Where would the liability lie?

The fieldwork agency should request a documented justification from the agency of the reasons for not defining the client as a data controller. It would be advisable if the agency's view on respective roles was documented too. The ICO have pointed out that they consider this low-risk decision making and not a priority enforcement area.

Please see our various updates on naming the end client as data controller - you'll find the most recent in the Privacy & Data Protection section.

If an end client has provided a list for sampling, does their name have to be revealed to the respondent even if the list is only used for the purposes of matching to a panel?

If the end client is a data controller then they would have to be named. When personal data is not obtained directly from the individual, the individual must be informed of the source of their personal data. Consequently, this means identifying the end client company if they provided the names even if the names are supplied via a third-party list supplier. So, the end client must be named as the source even when the names were supplied by a third party directly – as the end client initiated the supply. The list supplier should also be named as well to be as transparent as possible.

Do we have to name the commissioning client company if we receive or transfer personal data to them?

To secure informed consent the recipients or categories of recipients of personal data must be named, so, for example, the commissioning client must be named if they receive non-anonymised recordings of respondents participating in MR. The names of individuals viewing it do not have to be shared but the types of people do.

In addition, when the data is not obtained directly from the individual, the data subject must also be informed of the source of the personal data, so, for example, if a list of potential respondents is provided by the commissioning client company they must be named.

In addition, in the end client is a data controller they must be named (regardless of whether or not they receive any personal data). For more on this consult our **Privacy & Data Protection** resource: in particular the *Consents for Market Research - what is required and when guide* and our *Naming the End Client Guide*.

The BHBIA's Legal and Ethical Guidelines state that the end client (usually a pharmaceutical company) has to be named in some market research circumstances but the ABPI Code of Practice says the

pharmaceutical company does not need to be named, why is the BHBIA's guidance different to the ABPI's?

Clause 9.10 of the ABPI Code states that market research material need not include the name of the sponsoring company. As 'blanket' guidance this is not correct, there are some circumstances where there is a legal requirement to name the pharmaceutical company (the market research end client). The ABPI Code is correct in that there is no ABPI requirement to name the company but that this does not mean there is never a need to name the company. Data protection law requires that the company is named if they are a) the data controller or b) the source of respondents' personal data or c) recipients of respondents' personal data. There is no need to name the company sponsoring the market research unless there is a prior legal requirement.

The BHBIA's guidance on data protection requirements and their impact on naming the client company is detailed within the BHBIA's Legal and Ethical Guidelines, in section E4.2

Definitions and roles

The MRS advise that audio data is always personal data however the BHBIA guidance states voice alone is not necessarily personal data. Why the difference?

The BHBIA's guidance within the *Legal & Ethical Guidelines* on whether voice alone should be considered personal data or not is as follows:

Personal data includes sound and image data e.g. non-anonymised audio and video recordings from which an individual could be identified. Image data will always be personal data, a voice alone, may or may not be. If an individual belongs to small universe e.g. they are a KOL and have a distinctive accent, then voice alone is likely to be an identifier; however a GP's voice with a non-descript accent listened to out of area isn't likely to be identifiable data in isolation.

The MRS has stated within their *Data Protection & Research: Guidance for MRS Members and Company Partners 2018*, that:

Researchers should always categorise photographs, audio recordings, video recordings and still images as personal data. The ease of technology in linking these to an identifiable person means that there is a higher risk of re-identification for this type of media.

Under the GDPR, personal data is described as follows:
'…any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;'

The BHBIA has consulted with the Information Commissioner's Office (ICO) on this. The ICO considers the GDPR definition to mean that if you have information that could allow you to identify an individual, either directly or indirectly or are reasonably likely to have the means to identify, either directly or indirectly, an individual, then data will be personal data. It does depend on the context, i.e. the data will not be personal data if you are not, or are unlikely to gain, other information that can be used to

identify an individual. Organisations will have to look at the specifics of their situation and reach a decision on this. The fact that voice recognition technology exists does not necessarily mean that it should be assumed it could be used within a research context; this is likely to be viewed as unreasonable and disproportionate.

So the ICO has confirmed that whether voice alone is personal data or not, is context specific i.e. it is not necessarily always personal data, it depends on the context (as illustrated in the example provided in the BHBIA guidance above). This has not changed with the introduction of GDPR/DPA 2018.

It may be that clients or agencies will choose to take an overall view that they will err on the side of caution and treat all voice recordings as personal data rather than assess on a project-by-project basis. But the BHBIA did not want to take a more rigid position than is necessary and can be justified by the law, whereas the MRS has taken a more conservative approach.

If organisations are members of both the MRS and the BHBIA, then the MRS's more demanding guidance should be followed.

Which data privacy notice should be shown to respondents in cases where more than one organisation is involved?

It depends on the precise circumstances, but you may need to show more than one privacy notice – for example the fieldwork agency's notice when you are recruiting, and the MR agency's notice within the questionnaire, if it's the MR agency who will actually be collecting the data on their servers.

If more than one agency is involved in research, whose responsibility is it to keep the consent records?

It probably should be the fieldwork agency as they are the respondent-facing organisation (but with the understanding that the MR agency may want to audit their records). This is in line with GDPR data minimisation principles as it avoids unnecessary duplication/transfer of data.

Is personal data on a website that is accessible (although not necessarily immediately obvious) but was posted for another purpose (e.g. attendee list) subject to GDPR?

The use of personal data for a secondary purpose is only allowable if there is a lawful basis for the processing e.g. consent has been given or a legitimate interest assessment has been carried out and this is considered an appropriate lawful basis. The secondary use of personal data for 'research' is considered a compatible purpose but the questions remains whether commercial market research or data analytics are 'research' (as defined by GDPR).

What data are considered to be personal and sensitive?

The GDPR definition of 'personal data' is:

- *The GDPR defines personal data as 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification*

number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; (Article 4)

- *Genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question. (Article 4)*
- *'Biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data. (Article 4)*
- *'Data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status. (Article 4)*
- *Special categories of personal data (previously sensitive personal data) - data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. (Article 9)*
- *The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes. (Recital 26)*

Special category (previously referred to as sensitive) personal data includes racial or ethnic origin, political opinion, religious beliefs, membership of a trade union, physical or mental health or condition, sexual life. Personal health data includes all data pertaining to health status which reveals information relating to past, current or future physical or mental health status e.g. disease, disability, disease risk, medical history, clinical treatment. It also includes genetic and biometric data.

Data which when combined could be personal data should be considered and treated as personal data.

Key points to note:

- Personal data may be made up of more than one piece of information e.g. a job title and a place of work together could identify an individual.
- Pseudonymised data will still qualify as personal data if you have the ability to reverse the pseudonymisation.

BHBIA

bhbia.org.uk

What are the roles of Data Controllers and Data Processors?

Data Controllers determine the purpose and means of data processing, so for example, if you influence the design of the work or you maintain a list of potential respondents you are a data controller.

Data controllers are:

- Responsible for and able to demonstrate compliance with GDPR
- Responsible for providing a point of contact for data subjects
- Determine if and conducts Privacy Impact Assessment if required
- Can audit processor

Data Processors process the data on behalf of the data controller, so if you only act on the instruction of others (such as a market research or fieldwork agency), you are a data processor.

Data processors must:

- Seek approval to appoint sub-processor
- Include GDPR obligations in sub-processor's contract
- Seek approval to transfer personal data out of UK/EU

Both Controllers and Processors must:

- Implement technical and organisational measures
- Make sure contracts contain the right detail
- Appoint Data Protection Officer if this is required
- Keep detailed records
- Build in privacy by design and default
- Have a legitimate basis for data processing
- Maintain and store data and records

If a company commissions market research from an independent agency and this agency then conducts all the work on their behalf (under contract) and supplies the company with only aggregated anonymised data (i.e. the company does not have access at any stage to any of the personal data collected by the MR agency), the client company is a data controller as is the agency.

Although the data which the commissioning company will see is anonymised and aggregated, the collection, storage and other processing of personal data is happening for the commissioning company's overall purpose – without this purpose the processing would not be undertaken at all. The MR agency is applying technical expertise to the selection, processing and interpretation of personal data meaning they would also be data controllers (e.g. making a number of decisions about who, what, where, when and how personal data is processed as part of the project including the application of MR methodologies and design of any questions/interviews).

British Healthcare Business Intelligence Association
Fountain Precinct, 4th Floor Orchard Lane Wing, Balm Green, Sheffield, S1 2JA
t: 01727 896085 • admin@bhbia.org.uk • www.bhbia.org.uk
A Private Limited Company Registered in England and Wales No: 9244455

Can the BHBIA advise us whether we are a data controller or not?

The BHBIA cannot advise members what role they play with regard to any data processing. We can only relay regulatory guidance and provide the information that will allow members to come to their own conclusion.

Determination of whether an organisation is a data processor, independent data controller or joint data controller will depend entirely on what role the organisation plays in determining the purpose and means of data processing or whether they are simply acting on instructions. It is important to be clear that joint data controllers do not have to have the same or equal responsibilities.

The MRS provides the following definition and guidance:

Joint controllers: Joint determination of the purposes and means of the processing of personal data. 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.

The MRS provides extensive guidance in their 'MRS Guidance Note - Controllers and Processors' available to members on the MRS website. Unfortunately, there is no further news from the ICO or the EDPB on the interpretation of the definition of 'data controller' and the implications of determining that the commissioning client company is a data controller.

Who is the ICO?

The ICO is the Information Commissioner's Office. The ICO is the UK data protection supervisory authority or regulator. The ICO is an independent body set up to uphold information rights in the UK. It is a non-departmental public body which reports directly to Parliament and is sponsored by the Department for Digital, Culture, Media and Sport.

Is the MR agency a data processor if the client dictates the purpose of collection/processing of personal data via a brief and the means of personal data collection/processing?

A data controller determines the purpose and means of processing and a data processor processes the data on behalf of the data controller.

If an agency is applying technical expertise to the selection, processing and interpretation of personal data they would be data controllers (e.g. making a number of decisions about who, what, where, when and how personal data is processed as part of the project including the application of MR methodologies and design of any questions/interviews).

So, generally, both the commissioning client company and the MR agency are data controllers, but in some circumstances an MR agency might be a data processor.

Is a fieldwork agency a controller if it conducts the interviewing?

This would depend upon what if any other role the fieldwork agency has played in the project. If the fieldwork agency carried out the interviewing alone and did not influence recruitment or guide/questionnaire design then they are likely to

be a processor however if they have influenced the way in which the work is done then they are more likely to be a controller. Only if an agency is applying technical expertise to the selection, processing and interpretation of personal data they would be data controllers (e.g. making a number of decisions about who, what, where, when and how personal data is processed as part of the project including the application of MR methodologies and design of any questions/interviews).

Who would be responsible for a regulation breach if there are two controllers?

Contracts should detail the respective responsibilities of joint controllers, the controller liable for a regulation breach will be the controller responsible for that part of the activity that led to the breach.

Does the size of an organisation determine the need to appoint a Data Protection Officer (DPO)?

No. There was talk of this being the case at one time before the finalisation of the Regulation but this did not make it into the final draft of the GDPR. Data controllers and data processors must appoint a Data Protection Officer (DPO) if - as a core activity - you carry out large scale systematic monitoring of individuals or large scale processing of special categories of data.

Risk and Privacy Impact Assessment

What triggers the need for a DPIA?

DPIAs SHOULD be carried out when:

- *The data processing might result in a high risk to the rights and freedoms of the individuals*
- *If you are not sure whether your data processing is high or low risk, you need to carry out a DPIA – if in doubt, carry one out!*

DPIAs MUST be carried out when:

- *Large scale processing of personal data at regional, national or supranational level; that affects a large number of individuals; and involves a high risk to their rights and freedoms*
- *Large scale processing of special categories of data (previously referred to as sensitive data)*
- *Using new technologies and the processing is likely to result in a high risk to rights and freedoms*
- *Automated processing, including profiling, that results in automated decisions having legal effects or similar significant impacts on the data subjects*
- *The GDPR defines profiling as any form of automated processing intended to evaluate certain personal aspects of an individual (e.g. personalised targeted direct mailings), profiling is not the same as market research segmentation.*
- *Systematic monitoring of a publicly accessible area on a large scale.*

BHBIA

bhbia.org.uk

Notification and contracts

We are already registered with the ICO as a data controller – do we need to now specifically notify them under GDPR requirements?

The new data protection fee replaces the requirement to 'notify' (or register), which is in the Data Protection Act 1998 (the 1998 Act). Although the 2018 Regulations come into effect on 25 May 2018, this doesn't mean everyone has to pay the new fee on that date. Controllers who have a current registration (or notification) under the 1998 Act do not have to pay the new fee until that registration has expired.

If you have a master data processing agreement with a client that defines them as a data controller, could you have a project-specific variation on this – i.e. could they take a different position for an individual project?

Yes, if there was specific circumstance that justified departing from the agreement. Ideally the master agreement would include a clause that catered for exceptions.

How do we demonstrate that sub-contractors are working within the GDPR rules?

Sub-contractors/processors that process personal data on behalf of a data controller or processor must be under contract. Their responsibilities should be detailed in the contract. The option to audit the policies and processes of sub-processors may be included in the contract. Sub-contractors like all other parties in the data processing chain are accountable and part of that means keeping records of their data processing activities.

How do we manage responsibilities for data gathered by third parties or passed to third parties?

Third party responsibilities should be defined and managed through contracts or third party agreements. For further details on the use of third party contracts please see the BHBIA's Guidelines for the Use of Secondary Data - Sharing of and External Use of Purchased Data Assets, available on the BHBIA website.

If the commissioning client company does not provide a contract, what should we do?

The GDPR does not state which party is responsible for providing the contract, it only states that there has to be a contract in place between controller & processor or between processor & processor. The contract does have to be signed off in some way by both parties.

Do you need to register yourself as a data controller and/or processor with the ICO if you are a freelancer?

The current notification requirements are as follows:

Most organisations that process personal data must notify the ICO of certain details about that processing. However, the Act provides exemptions from notification for:

British Healthcare Business Intelligence Association
Fountain Precinct, 4th Floor Orchard Lane Wing, Balm Green, Sheffield, S1 2JA
t: 01727 896085 • admin@bhbia.org.uk • www.bhbia.org.uk
A Private Limited Company Registered in England and Wales No: 9244455

- *organisations that process personal data only for:*
- *staff administration (including payroll);*
- *advertising, marketing and public relations (in connection with their own business activity); and*
- *accounts and records;*
- *some not-for-profit organisations;*
- *organisations that process personal data only for maintaining a public register;*
- *organisations that do not process personal information on computer.*

Exemptions are also available in relation to:

- *national security and the armed forces;*
- *personal data that is processed only for research, statistical or historical purposes;*

Latest information on exemptions:

https://ico.org.uk/about-the-ico/consultations/dcms-consults-on-data-protection-fee-exemptions/

Under GDPR, this is what we know at present about new notification requirements:

When the new data protection legislation/GDPR comes into effect next year there will no longer be a requirement to notify the ICO in the same way. However, a provision in the Digital Economy Act means it will remain a legal requirement for data controllers to pay the ICO a data protection fee.

Latest information on fee requirements:

https://ico.org.uk/for-organisations/data-protection-fee/

What terms/changes might we need to make to our contracts?

Expect contracts under GDPR to include:

- Details of specific processing - subject matter, duration, nature, purpose, type of data & type of data subjects
- Risk & DPIAs requirements
- Information necessary to demonstrate compliance
- Safeguards - technical & organizational incl. confidentiality
- Retention, return, deletion requirements
- Data breach notification
- Inspection & auditing requirements
- Liabilities, assurances & indemnities for legal action
- Respective responsibilities of joint controllers

Data processors need the data controller's written consent to appoint sub-processors e.g. freelancers – they must adhere to GDPR too, and processor's must have contracts with named sub-processors too.

GDPR is not clear about whether the obligation to include processor clauses in contracts falls on the controller, the processor or both. The GDPR simply says these clauses must be included - so it is possible that both the controller and the processor must ensure they are included.

Could GDPR requirements be detailed in a study protocol rather than the legal contract with the client if the contract refers to the protocol?

This would have to be established by lawyers/legal advice.

Legal bases and respondent rights

How should you handle the situation in which a respondent is completing a questionnaire on behalf of other family members – i.e. they are supplying others' personal data?

You need a lawful basis for collecting personal data. It may be that in this case you could combine consent (for the individual filling in the survey) with legitimate interest (for the other household members). You would need a legitimate interest assessment to document this – e.g. potentially this could include the argument that consent is not practical in this scenario, but this would then prelude the collection of any special category data about other household members.

Is it the expectation that when passing on DFU call data, the client will have obtained consent for this data to be passed to the agency for detail follow up purposes?

Passing on data does require a lawful basis. Consent is a potential basis (note: explicit consent is not necessary as this is not special category data), but in most cases it is more likely that the client will rely on legitimate interests. Generally clients are using this basis for processing CRM data, and it's logical that this would also apply to transferring data for MR purposes. It would be necessary for the pharma company to do a legitimate interest assessment to justify this – and we recommend that agencies ask the client to confirm in writing their legal basis before they transfer the data.

Does verbal consent need to be audio recorded?

No, verbal consent does not have to be audio-recorded. The ICO advises within its guidance that if consent is given orally, you should keep a note of this made at the time of the conversation - it doesn't need to be a full record of the conversation.

What must we do if an individual makes a subject access request and wants to see film footage they are included in?

Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed
- access to their personal data
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.

The right of access allows individuals to be aware of and verify the lawfulness of the processing. You must provide a copy of the information free of charge. However, you can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. Information must be provided without delay and at the latest within one month of receipt. You must verify the identity of the person making the request, using 'reasonable means'. In providing access you should only allow access to the individual's personal data and not that of other individuals' which may mean that the material has to be edited before access is provided.

How valid is 'informed' consent when the terms of consent are extensive?

Consent has to be clear, specific and granular but as the same time it also has to be concise, these requirements may conflict at times as we struggle to make sure all the information that is required to support informed consent is difficult to deliver clearly and concisely. The ICO have suggested that:

"You must clearly explain to people what they are consenting to in a way they can easily understand. The request for consent needs to be prominent, concise, separate from other terms and conditions, and in plain language.
If the request for consent is vague, sweeping or difficult to understand, then it will be invalid. In particular, language likely to confuse – for example, the use of double negatives or inconsistent language – will invalidate consent."

Is consent needed to store data that is publicly available?

No, assuming that no other (non-publicly available) data are added to it. However you would require a lawful basis such as legitimate interest.

What is the difference between asking not to be contacted and asking for your personal data to be erased?

Under GDPR individuals have a new right to erasure, also known as the right to be forgotten. This gives the individual the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals also have a right to restrict processing of personal data. When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in future.

If an individual asks not to be contacted for the purpose of market research they are exercising their right to restrict processing (not their right to erasure). It is important not to confuse the two different rights. Quite clearly if you are going to observe a request not to be contacted for the purposes of market research you will need to store some personal data to do this.

If an individual specifically asks that their personal data is deleted and that they are not contacted again, the conflict between the two requests should be pointed out and their consent to hold their personal data for the purpose of making sure they are not contacted for market research should be requested.

Lists of individuals that should not be contacted may be passed on to sub-contractors, the legal basis for this processing might be consent or legitimate interests.

Is consent the only lawful basis that can be used for the processing of personal data for market research or data analytics purposes or can legitimate interests be used?

There must always be a lawful basis for the processing of personal data and within market research consent is the most frequently used lawful basis but it is not the only available option and it may not always be the most appropriate. 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 of the client). 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.

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

The ESOMAR and UK Market Research Society (MRS) provide the same advice to their members (https://www.mrs.org.uk/pdf/EFAMRO_ESOMAR_MRS%20GDPR.pdf).

Indeed they explicitly state that: *In line with previous opinions of WP29 (under the current Data Protection Directive) market, opinion and social research on client's customers is) within the reasonable expectations of customers. So although research is not specifically mentioned in the GDPR as a legitimate interest (although direct marketing is) it is expected that market, opinion and social research activities will fall within this ground.*

Click here to also see a later MRS update.

The BHBIA's GDPR update on the *Legal Grounds for Data Processing* is available on the BHBIA website - Privacy & Data Protection section - and includes further detail on the use of legitimate interests as a lawful basis for data processing.

Data breaches

Can you give some examples of how companies might fail in terms of their accountabilities?

The accountability principle requires that you show how you comply with GDPR requirements, so failure to define responsibilities in contracts, to record data

processing activities such as consent processes and agreements, to have a breach handling process in place would all be examples of accountability failings.

Data security, retention and destruction, incl. record keeping

What if a company employee travels abroad with their laptop containing personal data – for example on holiday?

If the company is a data controller or data processor or the laptop held the personal data of data subjects, GDPR requirements must be met.

What is the situation with respect to organisations holding data on back-up servers and GDPR requirements (e.g. requirement to name them)?

If the company hosting the backed up data does not have access to it – because the agency holds the key to accessing the data, then they would not be considered to be 'processing' the data.

For how long should AE reports be stored by pharma companies after being reported by agencies?

There is no specific guidance on the length of time AE reports should be stored for, the same rule applies to retention of all personal data – it should be stored for as long as it is necessary (until the purpose for which it is held is redundant) or according to contractual terms.

Would a small business be expected to maintain the same standard of written documentation as a large enterprise?

If you have 250 or more employees, you must document all your processing activities. There is a limited exemption for small and medium-sized organisations. If you have less than 250 employees, you only need to document processing activities that:

- Are not occasional; or
- Could result in a risk to the rights and freedoms of individuals; or
- Involve the processing of special categories of data or criminal conviction and offence data.

See more details here:

Who needs to document their processing activities? | ICO

Are google password protected spreadsheets compliant?

The BHBIA cannot provide advice on specific hardware or software solutions. The security measures you put in place should take into account the:

- Threats to, value and sensitivity of the data
- Damage that could be caused to individuals if there is a security breach

- State of the art, the costs of implementation and the nature, scope, context and purposes of the data processing.

Consequently there is no one set of security measures or solutions that will suit all situations. For further general guidance on data security considerations within its GDPR Update on Data Security including Breaches and International Transfers, this is available on the BHBIA website.

Can you tell us about the hardware/software infrastructure requirements for secure data storage?

The BHBIA has provided some general guidance on data security considerations within its GDPR Update on Data Security including Breaches and International Transfers, this is available on the BHBIA website.

How long does consent need to be kept for?

There is no specific guidance on the length of time records of consent should be stored for but the same rule applies to retention of all personal data – it should be stored for as long as is necessary (until the purpose for which it is held is redundant).

Data retention period should be 'appropriate', how long is appropriate?

The GDPR does not provide any guidance on how long is appropriate nor are data protection regulators likely to issue any. Personal data should not be held for longer than is necessary, the period of time should be agreed between the data controller and data processor. This is not a new requirement and should apply to all stored personal data (i.e. that stored pre and post GDPR).

How do we reconcile the need to hold personal data for a minimal time with the need to hold source data for PV purposes for 7 to 10 years?

The need to hold personal data must be justified, it must be necessary. If the reason is for PV purposes this should be explained, justified, agreed and recorded.

With regards to deleting data, what if the data is in the 'cloud'?

When personal data must be destroyed, all copies, in all forms, in all storage facilities (including the cloud) must be destroyed.

Global projects and transferring data overseas

When the personal data of a non-EU citizen is processed by an EU based controller or processor, is the non-EU citizen covered by GDPR and do they have data subject rights?

If the controller or processor is established in the EU then they must meet GDPR requirements even if the data subject is a non-EU citizen based outside the EU. So if the personal data of a non-EU based individual is processed by an organisation based within the EU, the individual has data protection rights.

If we have to transfer personal data out of the EU, what information must we give the data subject?

Data subjects must be provided with details of any data transfer to countries without adequate data protection (generally countries outside the EEA). Privacy notices should include details of any transfer to a third country, the safeguards, means by which to obtain a copy of them and where they have been made available.

For global projects is it the global team's responsibility to ensure GDPR compliance or the individual EU affiliates?

It is the *organisation* that is either a data controller or a data processor (not an individual office or team). The commissioning client company may be a data controller and therefore responsible for demonstrating compliance with GDPR. It is up to the organisation to decide which office/team is accountable for compliance.

Does the GDPR affect organisations outside the EU?

The GDPR applies to processing of personal data by an organisation:

Established within the EU, or

Not established within the EU where the processing relates to:

- Offering goods or services, irrespective of whether a payment is required, to individuals within the EU, or
- Monitoring the behaviour of individuals to the extent that behaviour takes place within the EU

The UK GDPR is the UK's post-Brexit version of the EU GDPR. It has been incorporated into the UK Data Protection Act 2018.

Application to specific scenarios

In social media research/scraping, if you have identifiable pseudonyms that can be traced back, what the requirements under GDPR?

Identifiable pseudonyms are personal data so GDPR requirements apply. All the same rules apply to social media as to any other MR medium – so to be GDPR compliant you need to provide all the required information to the data subject at the first appropriate opportunity (or check if it's already in the social media site's T&Cs).

What are the implications of GDPR for adverse event reporting?

The GDPR will impact the processing of personal data for adverse event reporting in the same way that it impacts data processing for market research – the same requirements will apply.

Does GDPR apply to projects involving social media listening?

Yes, the GDPR will applies to all forms of data processing, all medium and all sources of data.

Will client companies be able to observe non-anonymised fieldwork in person without their organisation being named on the consent form?

When fieldwork is viewed in person live via a one-way mirror or sitting in you must tell respondents that the end client will observe them and respondents must consent to this beforehand. In this situation personal data isn't being transferred to the end client, so data protection legislation does not apply and so the end client may remain anonymous unless you are legally obliged to reveal their identity for another reason e.g. the end client is a data controller or the end client supplied the sample. Before fieldwork starts, you should agree and document the client position on whether you can reveal their identity to respondents if it's requested, and if it can be revealed, when – during or at the end of the interview. You should reflect this in screener and interview materials, so that interviewers can react appropriately. If the live viewing is carried out via video relay/streaming, with and without recording then data protection requirements mean you must name the organisation(s) viewing before transfer of the personal data takes place. So if for example, the end client is viewing fieldwork live via a video-stream the client's identity must be revealed before fieldwork as part of the information communicated to secure respondents' informed consent.

For observation of interviews - respondent consent - what exactly does 'include recipients' mean? How much detail is needed?

The GDPR requires that when personal data are processed, those organisations to whom personal data will be transferred are named in order to secure informed consent (to allow the transfer). The name of the organisation must be provided as well as the roles of the individuals/teams that will have access e.g. market researchers, marketing, drug safety personnel. Individuals do not have to be named.

When transcribing or translating video recorded interviews, do we need to check with the commissioning MR agency that the participant has given consent for a sub-processor to access their data?

No, specific consent for sub-processing is not required as long as the processor and sub-processor are contractually bound and data protection requirements are included in the contract.

Secondary data and profiling

What are the implications of the GDPR for the processing of secondary data that includes personal data?

Broadly speaking GDPR requirements are the same for the processing of secondary data for data analytics as for primary data for market research. The BHBIA recommends that those involved in data analytics processing secondary data:

- Audit systems and work out where you are processing personal data
- Risk assess your processes and if necessary complete privacy impact assessments
- Review contracts with third party controllers / processors and ensure there is adequate clarity regarding roles and expectations

For further detail and specific secondary data examples please see the 'Implications of GDPR For Data Analytics' presentation prepared and delivered by Matt Beckett on the 7 September 2017 at the BHBIA GDPR Seminar *Building the GDPR into every stage of your project* and available to members on the BHBIA website - **click here**

It is possible to 'profile' a HCP for targeting (e.g. on the basis of their prescribing behaviour) and use legitimate interests?

Legitimate interests can be used as the legal basis for the use or secondary use of personal data such as targeting. Whether this is appropriate or not will depend upon:

- Whether the processing is necessary and proportionate (this in turn must take into account whether any other legal basis is available)
- Balancing the subject's rights, freedoms and interests with the controller's interests
- Whether the purpose of the data processing (in our case MR) could be reasonably expected by the data subject
- Having a privacy notice stating the purpose/legitimate interest, which in our case is MR.