Guidance on the General Data Protection Regulation (GDPR) and data protection for social research

Market Research Society and Social Research Association

2020

ACKNOWLEDGEMENTS

We are grateful to Dr Michelle Goddard who drafted this guidance while at MRS.

Peter Mouncey, Debrah Harding and Camilla Ravazzolo (MRS) and Graham Farrant (SRA) commented on drafts and edited and prepared the final document.

Many thanks to the following for reviewing the draft:

- Kelly Beaver (Ipsos MORI)
- Bob Erens (London School of Hygiene and Tropical Medicine)
- Simon Holroyd (NatCen Social Research)
- Hayley Moore Purvis (Department for Work and Pensions)
- Dr Scott Summers (UK Data Service)

Thanks to the Information Commissioner's Office (ICO) for help and support.

This guidance is the sole responsibility of the MRS and SRA.

COVERAGE

This guidance covers, as comprehensively as possible, the United Kingdom. Specific national and local regulations will need to be taken into account by researchers in relation with the specificities of their projects.

A NOTE ON THE USE OF 'DATA'

Technically, the word 'data' is a plural noun, with 'datum' referring to a single data item. On this basis one should write, for instance referring to a collection of data, 'the data are available', rather than 'the data is available'. However it is now widely accepted as common usage to refer to collections of data in the singular form ('the data is'), and in this guide we follow that usage.

DISCLAIMER

This guidance is not legal advice and you should not rely on it as such. It does not guarantee compliance with any legislation. You should seek specific legal advice if needed.

CONTENTS

TABLES AND FIGURES

1 SUMMARY OF KEY POINTS

Research that uses or collects personal information about identifiable, living people must comply with data protection law, and ensure that the rights of 'data subjects' are protected.

The General Data Protection Regulation (GDPR) (EU) 2016 and the UK Data Protection Act (DPA) 2018 provide the framework for this, replacing the Data Protection Act 1998. The Act applies to all nations of the UK.

The sections of this guide cover the main aspects relevant to social research:

- There is a research exemption for some provisions (Sections 2 and 10 to 12).
- In a research context 'data subjects' are likely to mean research participants (Section 4).
- An important and early decision in the research process is to identify the data controller, the joint controller (if there is one), and the data processor. The controller and joint controller determine why and how personal data is processed. A processor carries out the processing on behalf of a controller (Section 5).
- Data controllers and joint controllers are responsible for determining the lawful basis or bases for the research, as well as other responsibilities (Section 6).
- Several lawful bases are available to data controllers for processing personal data. There is no hierarchy of bases and 'consent' may not always be the best choice. There are other bases that might be more appropriate, such as processing for 'task in the public interest' or 'legitimate interests'. But high standards of ethical behaviour in research apply, and whether or not 'consent' is the lawful basis for processing personal data, you must follow ethical guidance on informed consent (Section 7).
- Data processors have certain responsibilities (Section 9).
- The GDPR permits some flexibility with data processing that is necessary for 'scientific or statistical research purposes' and is 'in the public interest'. This applies to processing data; data subjects' rights and notice requirements; and special category data. This is known as the 'research exemption' (Sections 10 to 13).

2 SUMMARY OF RESEARCH EXEMPTION

There are some exemptions from some provisions of the DPA 2018. The 'research exemption' applies when personal data is processed for:

- Scientific or historical research purposes or
- Statistical purposes and
- Is 'in the public interest'

These terms are not defined in the Act.

Recital 159 of the GDPR states that ''scientific research purposes should be interpreted in a broad manner, including for example technological development and demonstration, fundamental research, applied research and privately funded research'.'

The Information Commissioner's Office website notes that the research exemption ''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]

This SRA/MRS guidance is for social researchers. It seems reasonable that, in principle, research on social topics could be considered as 'scientific' and 'in the public interest' and therefore eligible for the research exemption.

Note that the SRA/MRS definition of research that is scientific and in the public interest, **for the purposes of this guidance**, is that it must add to a body of knowledge, and be open to assessment. The research findings must be publicly available, together with a description of the methods and approaches used.

The research exemption will not necessarily apply to every research project you conduct. You need to check this on a case-by-case basis. Sections 10 to 12 of this guidance cover the exemption in detail.

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/.

2.1 What this means

The research exemption means that the following provisions of GDPR may not apply:

- The right of access
- The right to rectification
- The right to restrict processing and
- The right to object

There are also other provisions which cover processing for research purposes (Section 10).

3 INTRODUCTION

The General Data Protection Regulation (EU) 2016/679 (GDPR) sets out the principles, rights and obligations for most processing of personal data.

It does not apply to processing for law enforcement purposes, or to areas outside EU law such as national security or defence.

The Data Protection Act (DPA) 2018 sets out the framework for data protection law in the UK. It updates and replaces the 1998 Act, coming into effect on 25 May 2018. It sits alongside the GDPR, and tailors how the GDPR applies to the UK – for example by providing exemptions. It also sets the separate data protection rules for law enforcement authorities, extends data protection to some other areas such as national security and defence, and sets out the functions and powers of the Information Commissioner.

This guidance refers to the GDPR as implemented by the DPA 2018. We refer to the articles of the GDPR and sections of the DPA 2018as relevant.

The guidance reflects UK implementation of the GDPR. We highlight differences between the four UK countries in the text.

3.1 Background

3.1.1 Scope of this guidance

This guidance reflects best practice for social research based on the extensive experience of the MRS and SRA. It replaces the MRS--SRA Data Protection Act 1998: Guidelines for Social Research (April 2013).

It provides general guidance to help social researchers comply with data protection obligations.

It focuses on the general approach to data protection when conducting scientific research, and includes information about the research exemption. There's also general information about data protection concepts and requirements.

Research-specific advice is published by MRS and other institutions such as the UK Statistics Authority and university research ethics committees. We signpost to these as relevant.

You should consult the Information Commissioner's Office (ICO) website for updates, including interpretations of the data protection framework.

3.1.2 How to use this guidance

Most organisations which are commissioning or conducting social research have an individual, or department, responsible for ensuring that the organisation meets data protection requirements. This should be your first source of help. If research is not your or your organisation's core activity, those responsible for data protection may not be fully aware of how the legislation affects research, or the distinctions between research and other uses of personal data. This guidance will help you and your organisation make the right decisions when commissioning and conducting research.

We recommend you read the guidance in full.

You can also use it to find answers to specific queries. Use the checklist below to find out what you need to know at different points in the research cycle.

Figure 1: Data protection checklist

Commissioning and set-up

- ☐ Determine the roles of those involved in the project. Remember that you could be a controller, joint controller and processor in the same project (over different personal datasets). (See Section 5.)
    - Are you a controller/joint controller?
    - Are you a processor?
    - Are you a third party?
    - Do you have a contract?

Project design and execution

- ☐ Determine the purpose and use of the data
    - Is this explained in the privacy policies?
- ☐ Data controllers need to choose the most appropriate lawful basis for processing. (See Section 7.)
    - What is your lawful basis for processing personal data?
    - Can you use 'task in the public interest' as a public authority controller?
    - Do you need to have a processing condition for collecting special category data?
- ☐ Consider the type and scale of personal data being processed. (See Sections 10 and 11.)
    - Do you need to do a data protection impact assessment (DPIA)?
    - Do you need to consult with your data protection officer (DPO)?
- ☐ Understand the research provisions for scientific or statistical research purposes. (See Sections 10 to 12.)
    - Do the exceptions apply?
    - Can you use the exemptions?

Data collection, analysis and publication of findings

- ☐ Apply the data protection principles. (See Section 4.)
- ☐ Anonymise or pseudonymise data as early as possible in the process. (See Section 14.)
    - Do you have control mechanisms to prevent identifiers being reconnected with the data set?
    - Is there a legal agreement with the research client that prevents re-identification and controls access to the identifier key?
- ☐ Determine how the research results will be published.
    - Research seeking to use the exemptions applying to 'scientific research' must be in the public interest. As noted, 'public interest' is not defined in law. Making the results and methodology publicly available is one way of demonstrating that the research is in the public interest.
    - Does the publication approach match any confidentiality assurances given to participants?
    - Has any personal data been anonymised?

Data retention and disposal

- ☐ Ensure data retention and disposal principles match the assurances given to participants at collection. (See Section 4.)
- ☐ Securely store and/or dispose of research materials.

4 DATA PROTECTION REQUIREMENTS

The DPA 2018 sets out requirements for processing personal data to protect individuals' personal information.

Requirements include:

- Enshrining privacy by design and default
- Conducting data protection impact assessments (DPIAs)[2]
- Keeping comprehensive data processing records
- Mandatory reporting of data breaches

4.1 Data protection principles

General privacy principles are at the centre of the framework – see Table 1 below.

Table 1 Data Protection Principles for Researchers

DPA 1988 Principle	GDPR principle/concept	Meaning under Art. 5(1) GDPR	Key points for researchers
Principle 1 – fair and lawful	*Principle (a) Lawfulness, fairness and transparency.*	Processed lawfully, fairly and in a transparent manner.	• Choose an appropriate lawful basis and ensure reflected in privacy notice. • Inform participant about how the research data will be used • Ensure data processing abides by the information and assurances provided
Principle 2 - purposes	*Principle (b) – Purpose limitation.*	Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be	• *Research provision:* If you can establish that further processing is necessary for archiving, scientific, statistical or historical research purposes then the personal data can be used for this purpose

DPA 1988 Principle	GDPR principle/concept	Meaning under Art. 5(1) GDPR	Key points for researchers
		considered to be incompatible with the initial purposes.	
Principle 3 - adequacy	*Principle (c) Data minimisation.*	Data should be adequate, relevant and limited to what is necessary for purposes for which they are processed.	• Limit data collection to the data required for a research project/exercise
Principle 4 – accuracy	*Principle (d) - Accuracy.*	Accurate and, if necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.	• Take reasonable steps to ensure that any inaccurate personal data is quickly erased or rectified. *Research exemption:* the right to rectify inaccurate data can be challenged if the data is processed for research purposes and safeguards are in place
Principle 5 – retention	*Principle (e) - Storage limitation.*	Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.	• Retain personal data for reasonable but generally short periods and establish and follow retention period(s) based on proposed use of the data • If acting as controller/joint controller on a research project, inform clients about the retention period • Define retention periods according to each research project and periodically review and revise the retention period • *Research exemption:* personal data processed for archiving, scientific, statistical or historical research purposes can be kept indefinitely subject to safeguards

DPA 1988 Principle	GDPR principle/concept	Meaning under Art. 5(1) GDPR	Key points for researchers
Principle 6 – rights	*No principle – separate provisions on individuals rights are included in chapter 3 of the GDPR.*		
Principle 7 – security	*Principle (f) – Integrity and confidentiality (security).*	Processed in a manner that ensures technical and organisational measures to guard against unauthorised or unlawful processing, loss, damage or destruction.	• Take steps to ensure security of the personal data by considering risk analysis, organisational policies, and physical and technical measures and use measures such as pseudonymisation and encryption as necessary
No equivalent provision	*Accountability principle.*	Organisations are responsible for, and must be able to demonstrate compliance with, the principles.	Incorporate and document all accountability measures such as: • Use of DPIAs for high-risk processing • Documentation including internal records of processing activities; the roles and responsibilities of parties involved in a research project; and particularly whether the researcher and their client are controllers, joint controllers, processors or third parties; lawful basis applied to the research project • Data breach records reflecting both mandatory notification regime and breaches not required to be reported to ICO • Appointment of DPO (or documented rationale for non-appointment)
Principle 8 – international transfers	*No principle – separate provisions on international transfers are included in chapter 5 of the GDPR.*		

DPA 1988 Principle	GDPR principle/concept	Meaning under Art. 5(1) GDPR	Key points for researchers
No equivalent	*Data protection by design and default.t*	Design and conceptualise data collection exercises to actively enhance privacy. Embed privacy in organisational practices, policies and procedures, including access controls and minimising data collection.	• Plan at the research design stage how best to protect the personal data of participants. Establish technical and organisational measures to implement the data protection principles and safeguard individual rights

In summary, the research exemptions (for scientific, historical or statistical research) are:

- Storage limitation: data processed for archiving, scientific, statistical and historical research purposes can be kept for longer subject to safeguards
- Purpose limitation: further processing is allowed for archiving, scientific, statistical and historical research purposes

See sections 10 to12 for more information about the research exemption.

4.2 Data subjects' rights

A key objective of the GDPR is to provide enhanced protection of personal data. It gives individuals extensive rights. Research participants can ask for their data or for it to be rectified or deleted. In certain circumstances they can ask for their data to be given to another organisation, and object to processing their personal data.

Data subject rights are set out in Table 2 below.

There is more about exemptions to these rights in a research context in Sections 10 to12 and Table 4. In a research context the specific criterion is that application of the right would prevent or seriously impair the achievement of the research purpose. In considering whether to apply researchers need to think about research integrity and reproducibility, other legal requirements, resource implications and the impact on scientific validity.[3]

[3]See further guidance from the Health Research Authority on exemptions: https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-detailed-guidance/data-subject-rights-and-research-exemptions/

Table 2 Rights of individuals under DPA 2018/GDPR

Right	Explanation	Limits to application
Right to be informed	Provision of extensive information to data subjects before processing of personal data such as who is processing the data, purpose of the processing, where the personal data came from; data subject rights, contact details of controller/joint controller, retention period, categories of data held and recipients. This will generally be provided through a privacy notice.	If information is not collected directly from data subjects, and the data subject already possesses the information or providing the privacy information would be impossible or would involve a disproportionate effort, then you do not have to inform individuals directly. In that regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration. In these circumstances DPIAs must be carried out in order to identify and mitigate the risks associated with your further use of the personal data. The information should still be made publicly available in a privacy notice.
Right of access	Right to access personal data about them (within 30 days and for free) includes a right to a copy of the personal data and access to information about the processing. It must be possible to make electronic subject access requests.	Data can be withheld if disclosure would adversely affect the rights and freedoms of other data subjects. Also, if the requests are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: (a) charge a reasonable fee taking into account the administrative costs or (b) refuse to act on the request. *Research exemption:* exemption can be applied if safeguards are in place; and the results of the research or any resulting statistics are not made available (including to other data controllers) in a form which identifies the data subject.

Right	Explanation	Limits to application
Right to rectification (of inaccurate data)	Right to have inaccurate records of personal data corrected. This can include having incomplete personal data completed by means of a supplementary statement.	Controllers can refuse to comply with a request for rectification if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. *Research provision:* right does not apply if it would seriously impair the purposes for which the data was gathered. The controller should carry out a balancing exercise to assess the effort involved to provide the information to data subjects against the impact and effects on the data subject if they are not provided with the information.
Right to erasure ''to be forgotten''	Right to erasure of information in specific circumstances. The controller also has an obligation to inform other controllers to also delete the personal data. This is not an absolute right. It is a complex right in terms of the applicable situations and exemptions. The right applies if: (a) Relying on legitimate interests as basis for processing, the individuals have objected and there are no overriding legitimate grounds to justify processing (b) Data is no longer needed for purpose for which it was collected (c) Consent is withdrawn and there is no other basis for processing (d) Data is being processed for direct marketing purposes and the individual objects to that processing	Right can be restricted: • If the lawful basis for processing is 'public task' • For archiving or research purposes • Necessary for freedom of expression or information • Public interest in the area of public health • Fulfilment of legal claims *Research provision:* right does not apply if data is processed for scientific/statistical research purposes and upholding the right would seriously impair the purposes for which the data was gathered. However if 'consent' is the lawful basis for processing the data involved and the data subject withdraws this consent, the data will need to be erased even if this is likely to render impossible or seriously impair the achievement of the objectives of that processing.

Right	Explanation	Limits to application
	(e) Data has to be erased to comply with a legal obligation (f) Personal data is being unlawfully processed (i.e. in breach of the lawfulness requirement of the first principle) (g) Data is being processed in connection with online service offered to a child	
Right to restrict processing	Right to request that processing be restricted which is applicable in certain circumstances. This is a more limited right than the right of erasure. It allows controllers to quarantine data i.e. refrain from using it • Accuracy of data is contested: can restrict use for as long as takes to verify accuracy • Processing is unlawful and data subject requests restriction (rather than erasure) • Where no longer needed for original purpose but required to establish, exercise or defend legal rights • During period considering an erasure request and seeking to verify whether there are overriding grounds to keep it.	You can refuse to comply with a request for restriction if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. *Research exemption*: right does not apply if data is processed for research purposes and safeguards are in place.
Right to data portability	Right to request personal data be provided in usable, transferable format to allow data to move between platforms or suppliers. The right applies if: • The processing is carried out electronically	Applies only to data collected by controller by consent or contract and the processing is carried out by an automated means. Right likely to be used more widely in sectors such as energy or telecommunications where it can be used to help data subjects find a better

Right	Explanation	Limits to application
	• The data was given directly to the controller by the data subject and • Processing is on the basis of either consent or contract	deal. May also be applicable to panel research companies.
Right to object to processing	Right to object to processing based on legitimate interests or public task.	Controllers do not need to comply if processing is for legal claims or based on compelling legitimate interests which override the interests of the individual, but burden of proof is on the controller to show there are compelling grounds for the continued processing. *Research exemption*: this right does not apply if data is processed for research purposes and safeguards are in place; and the lawful basis for processing is 'public task'. Always consider what participants have been told about withdrawing from the study and the ethical considerations of relying on the exemption to this right.
Right to withdraw consent	Must be as easy to withdraw consent as to give consent.	Continuation of current ethical practice. If using 'consent' as the lawful basis then there is no exemption to the right to withdraw consent.
Right not to be evaluated by automated decision-making	Right not to be evaluated/subject to automated decisions where decision has legal or significant effects. If a decision is made based solely on automated processing (such as by an algorithm) then the data subject has the right to express their point of view, contest the decision and ask for human involvement.	Right does not apply if the decision is based on explicit consent; necessary for a contract; authorised by European Union or Member State law. In a research context this is unlikely to be relevant to researchers as they do not typically make decisions about data subjects.

4.3 Identifying the client

Transparency is a fundamental principle of the GDPR and DPA 2018. Research participants must be given full information. This will generally include the name of the commissioning research client or research sponsor.

Commissioning research clients or sponsors must be named if they are:

- Controller or joint controller[4] of the research project
- The source of personal data for the research project.[5] If personal data has been obtained indirectly (i.e. not directly from the data subject) then the source of the data must be disclosed. A commissioning client who provides a sample of their customer database for research purposes will need to be named.

Recipients or categories of recipients of personal data, whether or not they are a data controller for the research, must also be named.

In order to meet transparency requirements, you should examine the facts of the case and the legal requirements on naming the parties. Some research organisations adopt a layered transparency approach, naming the client later in the data collection project, while providing an opt-out to the research participants. You should use this risk-based approach sparingly. If you adopt it, the controller should conduct a DPIA to assess privacy risks and ensure that assurances and opt-outs are given to participants.

4.4 Information requirements

The GDPR places much higher requirements on transparency of the information provided to individuals. The transparency principle applies throughout the data processing lifecycle (not just for collecting data) covering activities such as updating individuals about changes to processing or personal data breaches.

Articles 13 and 14 of the GDPR set out the information you must give participants. This is usually be done through a privacy information notice (also known as a privacy notice or fair processing notice) that states:

- Who you are
- What you are going to do with the information
- Who you will share it with
- The lawful basis for processing personal data

See Table 3 below for a summary of the requirements.

[4] GDPR Article 13(1)(a); Article 13(1)(e).
[5] GDPR Article 14(2).

Table 3 Information requirements when collecting data directly or indirectly from data subjects[6]

What information must be supplied?	Direct collection of data from data subjects	Indirect collection of data about data subjects
Identity and contact details of the controller (and if applicable, the controller's representative) and the DPO	✓	✓
Purpose and the lawful basis for the processing	✓	✓
The legitimate interests of the controller or third party, if applicable	✓	✓
Categories of personal data		✓
Any recipient or categories of recipients of the personal data	✓	✓
Details of transfers to any country outside the UK and EU, and safeguards	✓	✓
Retention period or criteria for determining the retention period	✓	✓
The existence of each of data subject's rights	✓	✓
The right to withdraw consent at any time, if relevant	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source of the personal data and whether it came from public sources		✓
Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	✓	

[6] ICO Guide to GDPR: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/.

What information must be supplied?	Direct collection of data from data subjects	Indirect collection of data about data subjects
The existence of automated decision-making, including profiling and information about how decisions are made, the significance and the consequences		
When should information be provided?	At the time the data is obtained.	Within a reasonable period of having obtained the data (within one month) If using the data to communicate with the individual, at the latest, when the first communication takes place or If disclosure to another recipient is envisaged, at the latest before the data is disclosed.

There is a UK Data Archive template for informing research participants at:

https://ukdataservice.ac.uk/media/622375/ukdamodelconsent.doc

4.4.1 How should the information be provided?

Informing participants using layered and blended formats (which actively provide some information and make other information accessible while using a range of techniques) is likely to be the most effective approach. You should ensure that information is:

- Written or conveyed in clear language and in an accessible form
- Tailored to the audience
- Age-appropriate
- Adapted to the communication channel (e.g. mobile, online, telephone)

Avoid using qualifying words such as 'may' so that participants are clear about your intentions. Regulatory guidance states that 'will' is clearer.

Use a combination of online and offline/written and oral methods to inform participants: videos, infographics, icons, cartoons, help centres, FAQs, telephone, human interfaces and chat bots.

4.4.2 Information you must actively provide or have available for participants

Researcher must ensure that relevant information is accessible to research participants.

- On the "what": you will need to decide what's most important to provide upfront and what can be available to find. This approach, also known as layering of information, allows you to assess which information is most relevant to provide immediately in terms of fairness and privacy risks (e.g. data controller, purposes, transfers, re-contact, ctc.) and what, although still fundamental, can be provided in another medium (e.g. privacy policy on a website)
- On the "who": you will need to assess which party is most appropriately placed to send invitations (e.g. client, controllers, research agencies, joint controllers etc.)

There might be exemptions to the provision of these information. As the ICO website states:

- 'The individual already has the information – You must be able to demonstrate [this].
- Providing the information to the individual would be impossible – You need to be able to show that it is impossible, not just inconvenient. This is most likely to occur if you do not have any contact details for individuals and have no reasonable means to obtain them. If you determine that providing privacy information to individuals is impossible, you must publish the privacy information (e.g. on your website), and you should carry out a Data Protection Impact Assessment (DPIA)
- Providing the information to the individual would involve a disproportionate effort – You must be able to show that the effort … is not warranted by the impact on individuals. To rely on this exception, you must make (and document) an assessment of whether there is a proportionate balance between the effort involved for you to provide individuals with privacy information

and the effect that your use of their personal data will have on them. The GDPR says (particularly if you use personal data for archiving or research purposes) you should take into account:

- the number of individuals involved;
- the age of the personal data; and
- any appropriate safeguards you have adopted.

If you determine that providing privacy information to individuals does involve a disproportionate effort, you must still publish the privacy information (e.g. on your website), and you should carry out a DPIA.'

4.5 Rights of individuals under the Freedom of Information Act 2000

The Freedom of Information Act (FOIA) 2000 creates a right of access to official information and places a duty on public authorities to publish information. The Act became law on 1 January 2005 and must now be interpreted in light of the DPA 2018 and the GDPR. The ICO will issue additional guidance on this area but researchers should note that the definition of personal data and sensitive personal data have changed, as have the data protection principles and the rights of subject access, which will be reflected in the approach to interpretation of the FOIA.[7]

While the Information Commissioner is the regulator for the DPA for England, Wales, Scotland and Northern Ireland, the ICO's powers covering the FOIA apply to only England, Wales and Northern Ireland. The Scottish Information Commissioner is responsible for the FOIA within Scotland.

The difference between the FOIA and the DPA is that the DPA enables individuals to gain information about themselves whereas the FOIA enables individuals to gain information about public authorities. If a person wants to gain information about themselves, they should make a subject access request. If an individual makes a request for information that includes someone else's personal data, then the organisation will need to balance the openness and transparency required by the FOIA with the data protection access request. In most cases, however, this personal data would not be disclosed. Information in the public interest is not the same as information that is of interest to the public. FOIA requests are addressed to the public authority, if the FOIA directly applies, and researchers involved

[7] Further information about the FOIA: https://ico.org.uk/for-organisations/guide-to-freedom-of-information/?template=pdf.

in assisting with requests on behalf of a client generally respond through the client and not directly to the individual.

Research data and research projects are not exempt from the FOIA, but personal data collected in a research project may be exempt, so you cannot use this legislation to gather personal data about individuals. Such personal data should only be released if it does not breach the DPA.

Research project-related data and information might also be exempt if a public body judges it, (using a prescribed test process), to be in the public interest to withhold the requested information (e.g. commercially sensitive information). This decision must be justified. The Scottish Government, for example, requires tenderers to place commercially sensitive information into an annex and describe the harm that might result from disclosure or publication. Some public data, collected for example in statutory business research or the Census, is protected by other legislation.

Examples of research project information that might be made available under the FOIA include:

- Invitations to tender
- Unsuccessful tenders and their assessments (with commercially sensitive information removed)
- Details of successful tenders including pricing (with commercially sensitive information removed)
- Details of how a project is managed, progress reports and reports on contract management
- Questionnaires
- Reports based on the research
- Existing data that is available but not published in reports (there is no obligation to generate new information, for example from further analysis, to meet a request). This can be a summary

FOI legislation applies only to public bodies. Data that is of poor quality, from flawed methodologies, or not 'fit for purpose' is not usually exempt from FOIA disclosure.

5 DATA CONTROLLER, JOINT CONTROLLER OR PROCESSOR?

5.1 Determining and documenting roles in a research project

Those involved in a research project must know whether they are acting as a data controller (for their employer[8]), joint controller or data processor, in order to determine their legal obligations under the GDPR, and to reflect these in the contract between parties.

Who is a controller, joint controller, processor or third party is a question of fact rather than contractual stipulation. It is based on evaluating **who determines the purposes (the why) and the means (the how) of the processing, and the level of decision-making power.**

Data controllers:

Determine the purposes and means of processing personal data. If two or more organisations jointly determine the purposes and means they are joint controllers. If they independently determine the purposes and means they are independent controllers.

Data processors:

Process personal data on behalf of controllers.

5.2 Points to consider

Depending on the role in and level of decisions about processing personal data, researchers and research organisations may be controllers or processors or both. For example:

- A research supplier receiving a sample from a client may be a processor of that personal data and may then be the controller of survey data subsequently collected
- If a research supplier provides a client with identifiable responses from consenting participants, the client could be the independent controller of this personal dataset while the supplier remains controller of the research data
- Anyone processing personal data solely on another's behalf such as interviewing, transcribing, coding, analysing and translating is likely to be a processor

[8] Freelance independent researchers can be controllers on their own behalf if they are independently collecting data not on behalf of a client.

You should decide and allocate roles on a project-by-project basis.

Although a contract may specify that a party is a processor, a supervisory authority such as the ICO can determine on the basis of a review of the activities that the party is actually a controller with the respective statutory obligations and responsibilities. Also, such decisions do not rely on which party paying for services, but on which party has decision-making authority.

The GDPR places specific obligations on all parties in the research supply chain. This may include the commissioning client, research suppliers, sub-contractors and/or or freelancers such as recruiters and interviewers.

5.3 Role and responsibilities

The responsibilities of each party vary according to their role.
You need to know the role of each party within any research project in order to:

- Meet the data protection principles especially on transparency of processing
- Determine which legal obligations and liabilities under the GDPR are directly applicable
- Enable the parties to reflect the mandatory written contract terms demonstrating compliance with all requirements of the GDPR
- Establish and document who is responsible for responding to data subjects' requests (if there's more than one controller)

Specific but different obligations are placed on controllers and processors which are reflected in the contracts.

The responsibilities of data controllers are described in Sections 6 to 8.
The responsibilities of data processors are described in Section 9.

6 DATA CONTROLLERS: RESPONSIBLITIES

If you are a controller or joint controller you are responsible for ensuring that data processing – including any processing carried out by a processor on your behalf – complies with the GDPR. Controllers have the following responsibilities:

- **Compliance with data protection principles:** you must comply with the data protection principles listed in Article 5 of the GDPR
- **Individuals' rights:** you must ensure that individuals understand and can exercise their rights over their personal data. These include rights of access, rectification, erasure, restriction, data portability, objection and rights related to automated decision-making
- **Security:** you must ensure technical and organisational security measures to protect personal data
- **Choosing a processor:** you must ensure that you use only a processor who can guarantee technical and organisational measures that meet GDPR requirements for processing data
- **Processor contracts:** you must enter into a binding contract or other legal act with your data processors. These must contain compulsory provisions as specified in Article 28(3) of the GDPR
- **Notification of personal data breaches:** you are responsible for notifying the ICO (and other supervisory authorities) about personal data breaches, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals
- **Accountability and governance:** you must comply with GDPR accountability obligations, such as maintaining records, carrying out DPIAs and appointing a DPO
- **International transfers:** you must comply with the GDPR's restrictions on transferring personal data outside the EU
- **Co-operation with supervisory authorities:** you must co-operate with supervisory authorities such as the ICO, and support them to perform their duties
- **Data protection fee:** you must pay the ICO a data protection fee (unless an exemption applies)

If you are a joint controller then you must also determine who will carry out each controller obligation under the GDPR. (However, each controller is responsible for *complying* with all the obligations of controllers under the GDPR). This is especially important for how you will comply with individuals' rights and transparency obligations. You should include the agreed roles and responsibilities in the

information you give to data subjects (either in your privacy notice, or in your participant information sheets).

Non-compliance: the ICO can take action against both the controller and the processor for non-compliance. This can include investigation, being subject to corrective powers, administrative fines, and other penalties. Individuals can also bring claims directly against the controller and processor in court. The court may require the controller and processor to pay compensation for any damage caused by the processing (this includes non-material damage such as distress).

The ICO website has more details about these principles: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/.

7 DATA CONTROLLERS: CHOOSING THE LAWFUL BASIS FOR RESEARCH

7.1 Overview of lawful bases for research

7.1.1 Processing bases for personal data

Under the GDPR there must be a lawful basis for processing personal data. The options are:

- Performance of a task in the public interest or in the exercise of official authority
- legitimate interests of a controller or third party
- Consent
- Performance of a contract
- Compliance with a legal obligation
- Protection of vital interests

There is no hierarchy in this list – see Figure 2 below.

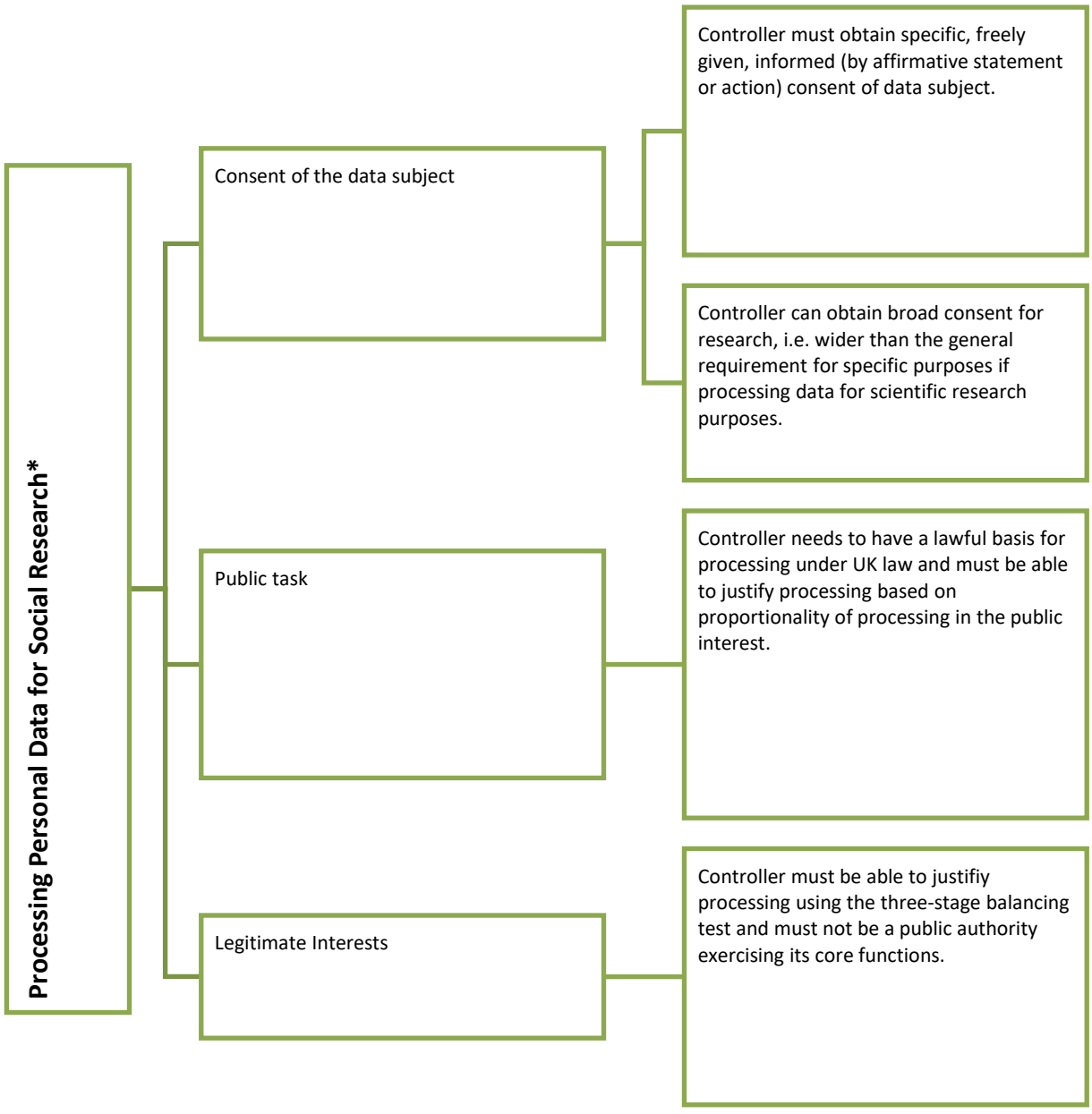
Data controllers must ensure that the right basis is chosen for data processing, and that this is described in data processing records.

For social research, one of the following bases is likely:

- Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller ('public task' for short)[9]
- Legitimate interest of controllers or third parties (this cannot be used by public authority controllers unless it is for non-core activities). (Research is likely to be considered as a core activity but will depend on the documents providing official authority, such as the university charter.)
- Consent that is freely-given, specific, informed and unambiguous (as long as there is not an imbalance of power between the public authority and the data subject)

[9] Article 6(3) and Recital 45 make it clear that this basis will apply only if the task carried out, or the authority of the controller is laid down in European Union law or Member State law to which the controller is subject. This basis can only be used if carrying out official functions.

Figure 2 Main processing bases for social research (Based on Articles 6, 9, 10 GDPR; Sections 8, 10; Sched. 1 DPA 2018



*The other legal bases are not discussed here as they are less likely to apply to social research: performance of a contract; compliance with a legal obligation; and protection of vital interests. 'Performance of a contract' may be relevant if there is a longer-term arrangement with an individual to participate in research in return for payment, such as a member of a research panel. Please refer to the ICO guidelines and MRS general guidance for more detail.

7.2 Using task in the public interest as a lawful basis

'Public task' provides a lawful basis when:

- processing is necessary for performing a task carried out in the public interest or in the exercise of official authority vested in the controller.

Public task applies if the research is 'in the exercise of official authority'. Section 8 of the DPA 2018 sets out a non-exhaustive list of functions, such as necessary for the administration of justice, parliamentary functions, statutory functions, governmental functions, and activities that support or promote democratic engagement.

This lawful basis covers public functions and powers that are set out in law. It is most likely to be used by public authorities but can also apply to any organisation that exercises official authority or carries out tasks in the public interest. The organisation does not need a specific statutory power to process personal data, but the underlying task, function or power must have a clear basis in law. Organisations with research as an incorporated or statutory purpose, including, for example, NHS organisations or universities, will find this basis useful. For example, for universities: university charter(s), Education Reform Act 1988, may be used as the lawful basis; for UKRI research institutes the Higher Education and Research Act 2017 may be used; for NHS trusts: legislation such as the National Health Service and Community Care Act 1990 may facilitate research.[10]

This condition can be satisfied when processing is necessary, reasonable and proportionate for the purpose of carrying out a public task. The organisation should assess whether it can lawfully use the public task basis, and document the justification for its decision.

7.2.1 Public task and necessary processing

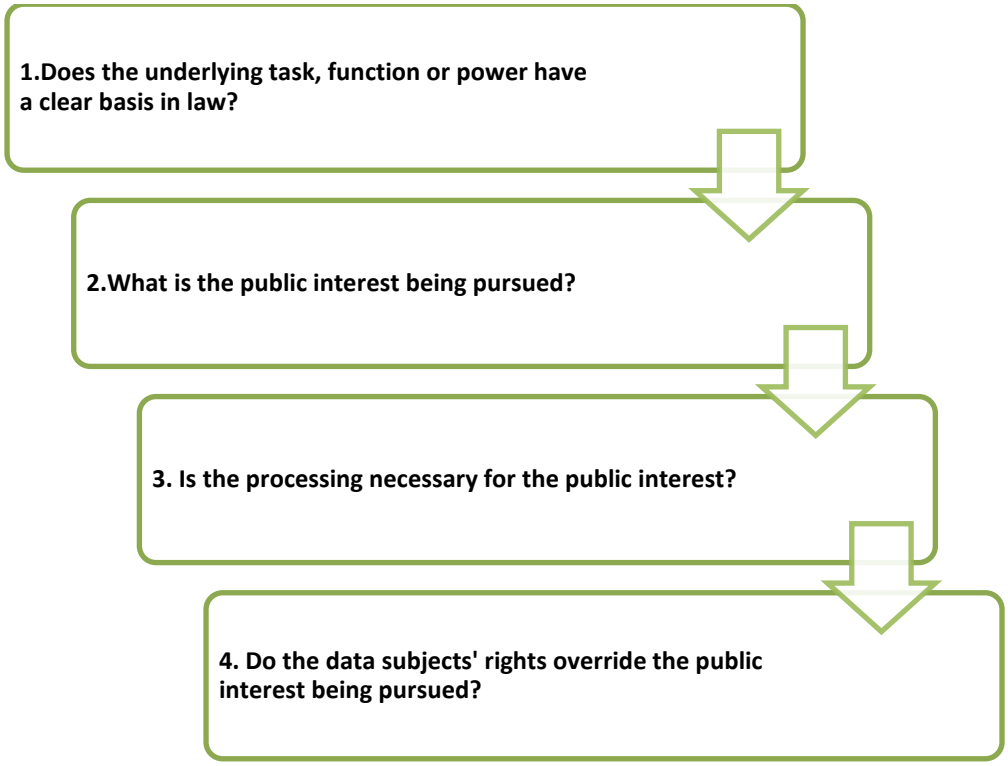
The processing must be necessary.

If the controller can reasonably perform the tasks or exercise the powers in a less intrusive way, this lawful basis does not apply. ICO states that, for accountability purposes, the data controller should be able to specify the relevant task, function or power, and identify its basis in common law or statute.

[10] See further for examples of sources of official authority in health and social care: NHS Digital

to the controller also needs to demonstrate that there is no other reasonable and less intrusive means to achieve the purpose.

Figure 3 Issues to consider in using public task



Organisations using 'public task' as a lawful basis must document and justify this with reference to the statutory public research purpose.

7.2.2 Public task and data subject rights

With public task, data subject rights are more limited thank with other lawful bases. For example, data subjects have a more limited legal right to object to processing, although for ethical reasons, potential and actual research participants must have the right to object and to withdraw from the research study.

If you are using exemptions to the data subject rights, you should explain to potential participants that an exemption may apply depending on the circumstances. You need to communicate this to participants clearly.

As with any research, you must always apply rigorous safeguards such as data minimisation, anonymisation or data security.

7.3 Using legitimate interests as a lawful basis

Legitimate interests provides a lawful basis when:

- processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party. It does not apply when such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular if the data subject is a child.

7.3.1 Determining the legitimate interest

Legitimate interests can be those pursued by the data controller (such as a research client) or by a third party. The type of interests that can qualify as legitimate are broad, and include processing for all types of research purposes (as well as commercial activities such as direct marketing). In determining whether legitimate interests can be used, organisations need to ensure that their interests are not overridden by the fundamental rights and freedoms of the data subject (see Section 4). You must take particular care in considering the rights of children and vulnerable participants.

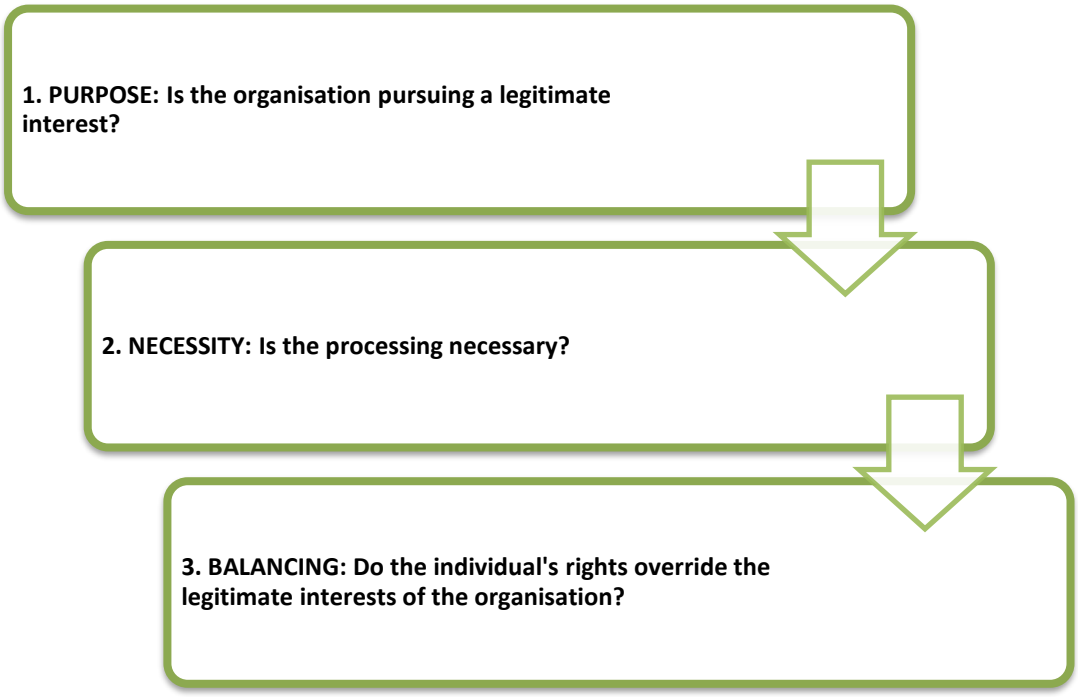
The legitimate interests may be those of:

- The researcher as a data controller, such as if a research agency re-contacts research participants for quality control purposes.
- A client as a data controller, such as when a researcher contacts the 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.
- A researcher as a third party wanting to use a database for research purposes

7.3.2 Applying the balancing test

Researchers using this processing basis will need to follow and document a three-stage approach. You must apply the process of considering, weighing interests and making a justified decision and document this in a Legitimate Interest Assessment.

Figure 4 Legitimate Interest Assessment



As with any research involving personal data you must always apply rigorous safeguards such as data minimisation, pseudonymisation, anonymisation or data security. You must follow standards set out in professional guidance, and recommendations on ethical practice (such as from ethics committees).

7.3.3 Legitimate interests for public sector organisations

Public sector bodies in the UK can use legitimate interests as a lawful basis when carrying out non-public tasks. An organisation is a public authority only 'when performing a task carried out in the public interest or in the exercise of official authority vested in it'. For example, the non-core functions of a university may include alumni relations and fundraising, for which legitimate interests can be used as a basis as appropriate. However, research for controllers which are public authorities cannot be based on legitimate interests, as research would likely be considered part of their core activities. The following online document from the GDPR Article 29 working party (2014) contains 26 examples to illustrate various scenarios in which data can be processed on the lawful basis of the legitimate interests of the data controller:

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

The scenarios highlight good practice as well as shortcomings and repay careful reading.

7.3.4 Further resources

See Article 29 Working Party Opinion on legitimate interests of the data controller under Article 7 of Directive 95/46/EC (April 2016): https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

7.4 Using consent as a lawful basis

Consent is a lawful basis when:

- the data subject has consented to the processing of their personal data for one or more specific purposes.

Informed consent is an important ethical principle in conducting research. This does not mean that 'consent' must be chosen as the lawful basis for processing participant data under GDPR. You can gather participant data for your study, taking ethical guidance on the rights of participants seriously, while not using consent as the lawful basis for processing.

When collecting and processing special categories of personal data, additional safeguards and conditions apply – see Section 13.

7.4.1 Informed consent

Consent may be given in writing, electronically or orally. Researchers using consent as the lawful basis for data processing must ensure that a participant's consent is:

- Freely-given
- Specific to the research purpose(s) (which you must explain to potential and actual participants)
- Informed
- An 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 indicate consent

You must keep records so that consent is documented. For example, if a participant gives consent over the telephone then you must keep a copy of the script and details of who consent was given to and when (date/time). Recordings of verbal consent are not mandatory but are preferable.

If consent is used as the lawful basis, then the participant has a right to withdraw that consent at any time. It must be as easy for them to withdraw consent as it is to give it. If they withdraw consent at a later stage of research, for example in a subsequent round of a longitudinal study, you need to remove all the data they provided.

Participants must consent by an affirmative action or statement. Opt-outs cannot be used. Therefore, if a research project includes an opt-out stage, for example to make an initial contact with sample members, you should use a different lawful basis for the research.

7.4.2 Use of broad consents for scientific research

In seeking consent for scientific research purpose(s), you need to meet all the standard general conditions for consent. However, if the research purpose(s) cannot be fully specified at the outset, then the data controller(s) should use transparent mechanisms to 'ensure the essence of the consent requirements. Guidance from the European Data Protection Board explains that this could include more general consent terms, seeking consent in stages before each phase of the research begins and supplying participants with a comprehensive research plan at the outset of the research. As with any research you must always apply rigorous safeguards such as data minimisation, anonymisation or data security.

7.4.3 'Consent' may not be a suitable basis for some research

With social research it may not always be possible to know at the outset all the future uses of the data being collected. Data controllers should consider whether a lawful basis other than consent is more suitable.

When research purposes cannot be fully specified, data controllers should ensure that the essence of the data subject rights to valid consent is served, including ensuring transparency and other safeguards.

8 DATA CONTROLLERS: FURTHER PROCESSING

Personal data must be collected for well-defined purposes and not further processed for additional purposes.

Exceptions to this are if the secondary use of the data is:

- Based on consent
- For scientific or statistical research purposes or
- Based on EU or Member State Law

Processing can also take place if it is compatible with original data collection purposes.

Further processing of data under Article 6(4) of the GDPR based on compatibility takes into account:

- Any link between the purposes for collecting the personal data and the purposes of the intended further processing
- The context in which the personal data have been collected, in particular the relationship between data subjects and the controller
- The nature of the personal data
- The possible consequences of the intended further processing for data subjects
- The existence of safeguards, which may include encryption or pseudonymisation

8.1 Based on consent

Personal data can be further processed if you obtain consent for the specific purpose 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 they need to seek new consent. There is no scope for processing for further 'compatible' purposes to inherit the original consent as a basis for processing.

So you must define as best you can any further, secondary purposes when collecting consent at the outset of the research project. If the research project is scientific or statistical research, and/or the lawful basis for processing is 'public task', it may be possible to provide additional information as the project progresses but you should not use this as a default option. See further information about using this lawful basis in Section 7.4.

8.2 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.

Some 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 of personal data (collected for another non-research purpose) using the legitimate interests of the data controllers/clients as the processing basis. In these circumstances, a research purpose is likely to be compatible with the original data collection and processing purpose.

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

Researchers must first check to see whether a research project can be carried out with de-identified or anonymised data. Special category data cannot be processed on the basis of legitimate interests unless there is an additional processing condition.

8.3 Based on scientific or statistical research purposes

See Sections 10.1 and 10.2.

9 DATA PROCESSOR RESPONSIBILITIES

If you are a data processor you have direct legal obligations to fulfil under GDPR, and are subject to regulation by supervisory authorities. Processors have the following obligations:

- **Controller's instructions:** you can process personal data only on the instructions of a controller, unless otherwise required by law
- **Processor contracts:** you must enter into a binding contract with the data controller. This contract must contain the compulsory provisions mentioned in Article 28(3) of the GDPR (http://www.privacy-regulation.eu/en/article-28-processor-GDPR.htm). You must comply with your obligations as a processor under the contract
- **Sub-processors:** you must not engage a sub-processor without the prior written authorisation of the controller. If authorisation is granted, you must ensure there is a contract in place with the sub-processor that has terms covering the protection of personal data equivalent to those terms in the contract between you and the controller
- **Security:** you must implement appropriate technical and organisational measures to secure personal data, including protecting against accidental or unlawful destruction, loss, or alteration, and against unauthorised disclosure of access
- **Notification of personal data breaches:** Iif you become aware of a personal data breach, you must notify the relevant controller immediately or without undue delay (data controllers have only a limited amount of time to report breaches to the ICO). You must also assist the controller in complying with its obligations regarding personal data breaches
- **Notification of potential data protection infringements:** you must notify the controller immediately if any of their instructions would lead to a breach of GDPR
- **Accountability obligations:** you must comply with certain GDPR accountability obligations, such as maintaining records and appointing a DPO
- **International transfers:** you must ensure that any transfer of data outside the European Economic Area (EEA) is authorised by the controller and complies with GDPR transfer provisions

Non-compliance: the ICO can take action against both the controller and the processor for non-compliance. This can include investigation, being subject to corrective powers, administrative fines, and other penalties. Individuals can also bring claims directly against both the controller and processor in court. The court may require the controller and processor may to pay compensation for any damage caused by the processing (this includes non-material damage such as distress).

10 USING THE RESEARCH PROVISIONS

Personal data processed for 'scientific or historical research purposes, statistical purposes or archiving purposes' in the public interest is subject to an exemption. Controllers must apply the exemption on a case-by-case basis and the applicability/necessity of use of the exemption should be a preliminary consideration in the research design phase.

Special rules have been developed for research in recognition of the importance of a strong science base and the fact that the use of personal data is critical in providing insights and ensuring quality and reliability in scientific research. It also supports the objective of achieving a European research area to support innovation and advancements in medicine, science and technology and to ensure the EU remains competitive in world markets.

The research exemption provides flexibility for processing for research purposes particularly for certain data subject rights and notice requirements. All researchers (whether based in the private sector, public sector, charity sector or academia) can use the exemption depending on the type of research being conducted.

Although this exemption affords researchers with a certain level of flexibility, most of the provisions of the GDPR still apply.

10.1 What is scientific research?

As noted in Section 2, scientific research purposes are not defined in the GDPR or DPA 2018, but the provisions make it clear that 'scientific research purposes should be interpreted in a broad manner, including for example technological development and demonstration, fundamental research, applied research and privately funded research'. [11]

The International Association of Privacy Professionals notes that the relevant GDPR recital:

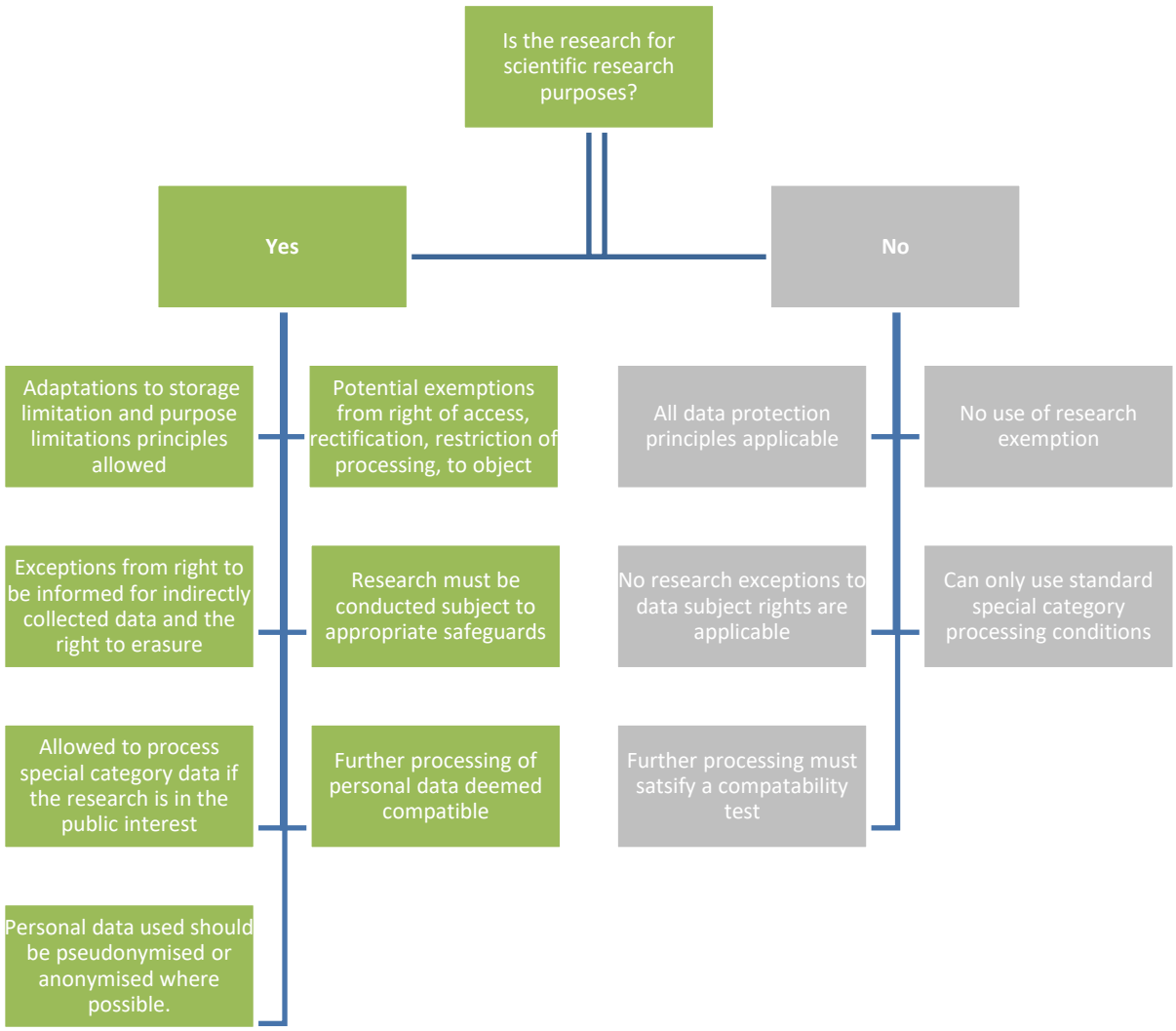
> 'cites Article 179(1) of the Treaty on the Functioning of the European Union, which promotes 'the objective of strengthening its scientific and technological bases by achieving a European research area in which researchers, scientific knowledge and technology circulate freely.' This suggests that although private research for technological development qualifies as research, there may be a requirement that the research be published or otherwise made available outside the private entity. An important interpretative question concerns the application of the research provisions to

[11] Recital 159 GDPR; Section 18 DPA 2018.

corporate contexts such as research for product improvement or marketing purposes, as opposed to 'big-r' research in academic institutions, which is geared at publication and contribution to generalizable knowledge.'[12]

The broad nature of the above definition seems likely to encompass much of social research.

Figure 5 Scientific research flowchart



---

[12] https://iapp.org/news/a/how-gdpr-changes-the-rules-for-research/.

10.2 What are statistical purposes?

Statistical purposes are defined in GDPR as 'any operation of collection and processing of personal data necessary for statistical surveys or for the production of statistical results.[13] Research that results in aggregate data, that is not used to support measures or decisions about an individual, is statistical research. The outputs of statistical research can also be used for other purposes including scientific research.

The definition of 'statistical research' broadly encompasses any research that collects, analyses and interprets data on a numerical basis. The key factor is that the data subjects are considered in combination, not individually, with findings described in terms of proportions of the sample. Any research carried out on this basis may be considered 'statistical' under GDPR.

See UK Statistics Authority guidance on using statistical purposes: https://gss.civilservice.gov.uk/policy-store/uk-statistics-authority-guidance-on-the-general-data-protection-regulation-gdpr/.

- UKSA Guidance on the Safeguards of Statistical Processing
- UKSA Guidance on the Provision of Information to Data Subjects
- UKSA Guidance on the Lawfulness of Processing for Statistical Purposes
- UKSA Guidance on Statistical Exemptions to the Data Subject Rights

10.3 What are historical research purposes and archiving?

Historical research purposes include 'research for genealogical purposes, bearing in mind that the Regulation does not apply to deceased persons'.

Archiving in the public interest recognises that there is a public interest in permitting the permanent preservation of personal data for the long- term benefit of society. It provides for various exemptions that apply to archiving by public, private or voluntary bodies.

There are other provisions that may be relevant to social researchers. These include freedom of expression and information. These are not covered in this guidance.

[13] Recital 162 GDPR; Section 18 DPA 2018.

11 WHAT IS THE PUBLIC INTEREST?

Public interest in the data protection framework is relevant to:

- Using 'task in the public interest' as a processing ground for personal data
- Using scientific research in the public interest as a condition for processing special category data
- Using substantial public interest conditions for processing special category data

11.1 Defining the public interest

For reasons of flexibility, public interest is not defined in information legislation. There is no specific definition of the public interest in the GDPR or DPA 2018. In passing the DPA 2018, the UK Government thought that the public interest would vary across sectors and should be defined in context.

This guidance explains the public interest test that you should apply to a research project.

In general, as noted by the ICO 'the public interest can cover a wider range of values and principles relating to the public good, or what is in the best interests of society'.[14] There is ICO guidance on public interest in its guidance on the FOIA and the Environmental Information Regulations 2004 (EIR).[15] For Scotland, there is guidance on Freedom of Information (Scotland) Act 2002 (FOISA) and Environmental Information (Scotland) Regulations 2004. There is also guidance on how the term 'public interest' is used in public law proceedings in UK courts. Public benefit requirements under the Charities Act 2011 indicate the elements of a public interest test.[16]

Public interest should represent collective interests, promote wider values than purely economic or market issues and take account of interests of all, including future citizens.

Public interest should cover research of wide benefit to society and the economy. For research to be defined as in the public interest, it must be of benefit to the society. Its main aim should be to inform society or provide some broader benefit to the public.

[14](ICO) PDF: The public interest test: Freedom of Information Act https://ico.org.uk/media/for-organisations/documents/1183/the_public_interest_test.pdf
[15] https://ico.org.uk/for-organisations/guidance-index/freedom-of-information-and-environmental-information-regulations/.
[16] https://www.gov.uk/government/collections/charitable-purposes-and-public-benefit

11.2 Public interest test for research

Suggested criteria for processing for research in the public interest are set out below. These are based on the public interest considerations and take into account spectrum of activity covered by scientific research.[17]

Public interest research purposes should focus on research activities that serve the public good and benefit society (and are not for personal or private gain). Examples include:

- Providing or improving evidence bases that support the formulation, development or evaluation of public policy or public service delivery; guiding decision-making with anticipated benefits for the economy, society or quality of life of people in the UK
- Significantly extending understanding of social or economic trends or events, either by improving knowledge or challenging accepted analyses
- Replicating, validating, challenging or reviewing existing research (including official statistics) in a way that leads to improvements in the quality, coverage or presentation of existing research

Research that is in the public interest can be carried out by controllers which are public authorities, commercial organisations, other non-commercial researchers, such as those based in university research centres, think-tanks, charities, or not-for-profit organisations.

[17] Research Code of Practice and Accreditation Criteria: https://www.gov.uk/government/publications/digital-economy-act-2017-part-5-codes-of-practice/research-code-of-practice-and-accreditation-criteria.

12 WHAT ARE THE SPECIFIC EXEMPTIONS FOR RESEARCH?

The research exemption is set out in Section 19 of the DPA 2018 which implements Article 89(1) of the GDPR.

Exemptions and exceptions from certain rights

Controllers processing personal data for scientific research purposes can use the following exemptions and exceptions from the GDPR provisions. You don't have to use them. But if you intend to, you must tell participants which rights you are exempting and on what grounds:

- Right of the data subject to object to processing of personal data (where necessary in the public interest)
- Right to restrict processing pending verification or correction
- Right to have inaccurate data rectified

The GDPR also provides for exceptions from provisions on the right to be informed and the right to erasure:

- Right of data subjects to exercise their 'right to erasure' is restricted if it is likely to significantly impair processing for scientific research purposes
- Limitations are placed on the right of data subjects to be informed (for indirectly collected data)

The DPA 2018 does not use the additional GDPR flexibility for the research exemption such as an exemption to the right of a child to be forgotten. Researchers must fulfil these rights when requested by a data subject.

Adaptations to data protection principles

The GDPR also limits the application of the purpose limitation and storage limitation principles so that researchers conducting scientific research can:

- Use personal data collected for other purposes than research
- Store personal data for longer periods. The ICO has stated that this means indefinitely. Decisions on retention should be documented with clear explanation of the rationale for the retention period

- Make isolated transfers of personal data to countries outside the EEA taking into account legitimate expectations of society for an increase in knowledge[18]
- Limit obligations on the level of information provided to data subjects in scientific research if it would involve a disproportionate effort

12.1 What safeguards must researchers meet?

Use of the research exemptions and exceptions is not automatic. You must:

- Consider the necessity of the processing
- Consider the extent to which compliance with standard data protection requirements would impair the processing purposes
- Meet the conditions and safeguards below

Safeguards to protect the rights and freedoms of data subjects

Under the DPA 2018 processing data must be exclusively for research purposes. The safeguards that need to be met include:

- Not for measures or decisions about the data subjects (unless necessary for approved medical research)
- No likelihood of substantial damage or substantial distress to any data subjects
- The research results are not made available in a way that identifies individuals

Adequate technical and security measures

Technical and organisational measures must be in place. For example:

- Data minimisation: you should collect only data that is necessary; minimise the number of participants; the amount of data per participant; and the degree of sensitivity of data collected and used
- Use of pseudonymised data or anonymised data where possible
- Access controls that ensure that only those who need to know are allowed access to personal data
- Encrypting the personal data

Researchers can achieve this by following internal governance mechanisms and taking advice from the DPO, if there is one.

[18] Transfers must follow the options set out in Article 44 and 49 of the GDPR.

12.1.1 What flexibility is there in providing information to data subjects?

Article 14 of the GDPR provides for exceptions to the requirement to provide privacy information in circumstances where the personal data has not been obtained directly from the data subject.[19] If you obtain personal data for scientific research from a source other than the data subject, you are exempt from the need to provide data subjects with privacy information only if doing so would be impossible or would involve a disproportionate effort.

- **Providing the information to the individual would be impossible**: situations in which it is impossible to provide privacy information to individuals are few and far between. This is most likely to occur if you do not have contact details for individuals and have no reasonable means to obtain them. If it's impossible to provide privacy information to individuals, you must take other measures to protect individuals' rights. Privacy information must be made publicly available and a DPIA must be carried out
- **Providing the information to the individual would involve a disproportionate effort**: to rely on this exception, you must assess (and document) whether there is a proportionate balance between the effort involved to provide individuals with privacy information and the effect that your use of their personal data will have on them. The more significant the effect, the less likely you can rely on this exception. Particularly if you use personal data for archiving or research purposes, you should consider:
    - The number of individuals involved
    - The age of the personal data
    - Any appropriate safeguards you have adopted

If providing privacy information to individuals is impossible or does involve a disproportionate effort, you must take other measures to protect individuals' rights. These include making the privacy information publicly available and carrying out a DPIA.

12.1.2 Do researchers have to meet all data subjects' rights?

Data subjects have several rights under the GDPR/DPA 2018 as set out in Table 1. However, there is some leeway for scientific research projects, as set out in Table 4 below.

[19] Additional exemptions include obtaining or disclosing is expressly laid down in law; serious impairment of objectives; confidentiality by virtue of a secrecy obligation.

Table 4 Data subjects' rights and research projects

	Task in the public interest	Consent	Legitimate Interest	Impact of research exemption on data subject rights
Right to be informed	Yes	Yes	Yes	Right can be restricted if researcher indirectly collects personal data or will require disproportionate effort.
Right to withdraw consent	N/A	Yes	N/A	No impact on this right if using consent.
Right to object to processing	Yes (but can be overridden if scientific research in the public interest).	No right to object to processing but can withdraw consent.	Yes (but can be overridden if scientific research in the public interest).	Exemption from this right available if processing necessary in the public interest. If processing has been based on public task then this will have been established. If the lawful basis for processing is different from this, the controller should document justification for the processing being necessary for a task carried out in the public interest. This can be demonstrated even if the lawful basis for your processing is not 'task in the public interest' and will allow the exemption to be used, and the data to be processed, even if a research participant withdraws from a study, provided that consent is not the lawful basis for processing. Always consider what participants have been told about withdrawing from the study and the ethical considerations of relying on the exemption to this right.
Right to access data	Yes	Yes	Yes	Right can be restricted if safeguards are in place and research results are not made available in a way that identifies individual. If a copy of the raw data that can identify the individual is available then they would still have a right of access.
Right to rectification of inaccurate data	Yes	Yes	Yes	Exemption from this right available.
Right to erasure of data	No	Yes	Yes (but balancing test to be carried out by controller	Right can be restricted if likely to significantly impair processing for scientific research purposes and processing not based on consent.

	Task in the public interest	Consent	Legitimate Interest	Impact of research exemption on data subject rights
			to determine if overriding legitimate ground for processing).	
Right of a child to be forgotten at age [18]	Yes	Yes	Yes	No impact on this right.
Right to restrict processing pending verification or correction	Yes	Yes	Yes	Exemption from this right is available.

12.1.3 Can participant research data be shared?

Personal data that is part of a research study can be archived and/or shared with others in line with the data protection principles in the DPA. The DPA also applies to pseudonymised data (but not anonymised data) but you need to tailor the approach.

If personal data is to be shared, then this must be done in a transparent manner and in line with the assurances provided to participants. If assurances are given about confidentiality these should be met, and data shared only with participant consent or if required by a legal obligation or gateway (such as, in England and Wales, sharing confidential patient information under Section 251 of the National Health Service Act 2006 and its current Regulations, the Health Service (Control of Patient Information) Regulations 2002.) In all instances there must be proper processes for managing and overseeing access.

For detailed guidance on data sharing, see the UK Data Service guidance:

- https://reshare.ukdataservice.ac.uk/
- https://www.ukdataservice.ac.uk/manage-data/plan/how-share.aspx

13 PROCESSING CONDITIONS FOR SPECIAL CATEGORY DATA

Personal data categorised as special category data is data on religious or philosophical beliefs, health, racial or ethnic origin, trade union membership, political beliefs, sex life or sexual orientation, genetic data and biometric data (including photos when used for uniquely identifying a natural person) of data subjects.[20]

In addition to a lawful basis (see Section 7), processing special category data also needs to meet one of the additional conditions for processing under Article 9 of the GDPR or Schedule 1 of the DPA 2018. Relevant conditions for social research include:

- Do you have the explicit consent of the data subject?
- Has the data been made public by the data subject?
- Are there reasons of substantial public interest including equal opportunities monitoring etc. for processing, as set out in Figure 6 below
- Is the processing for historical, archival, scientific or statistical research in the public interest?

There are limited grounds for processing personal data about criminal convictions or offences. You must either process the data in an official capacity or meet a specific condition in para. 1, 2 and 3 of Sched.1 DPA 2018 and comply with the additional safeguard in the DPA.

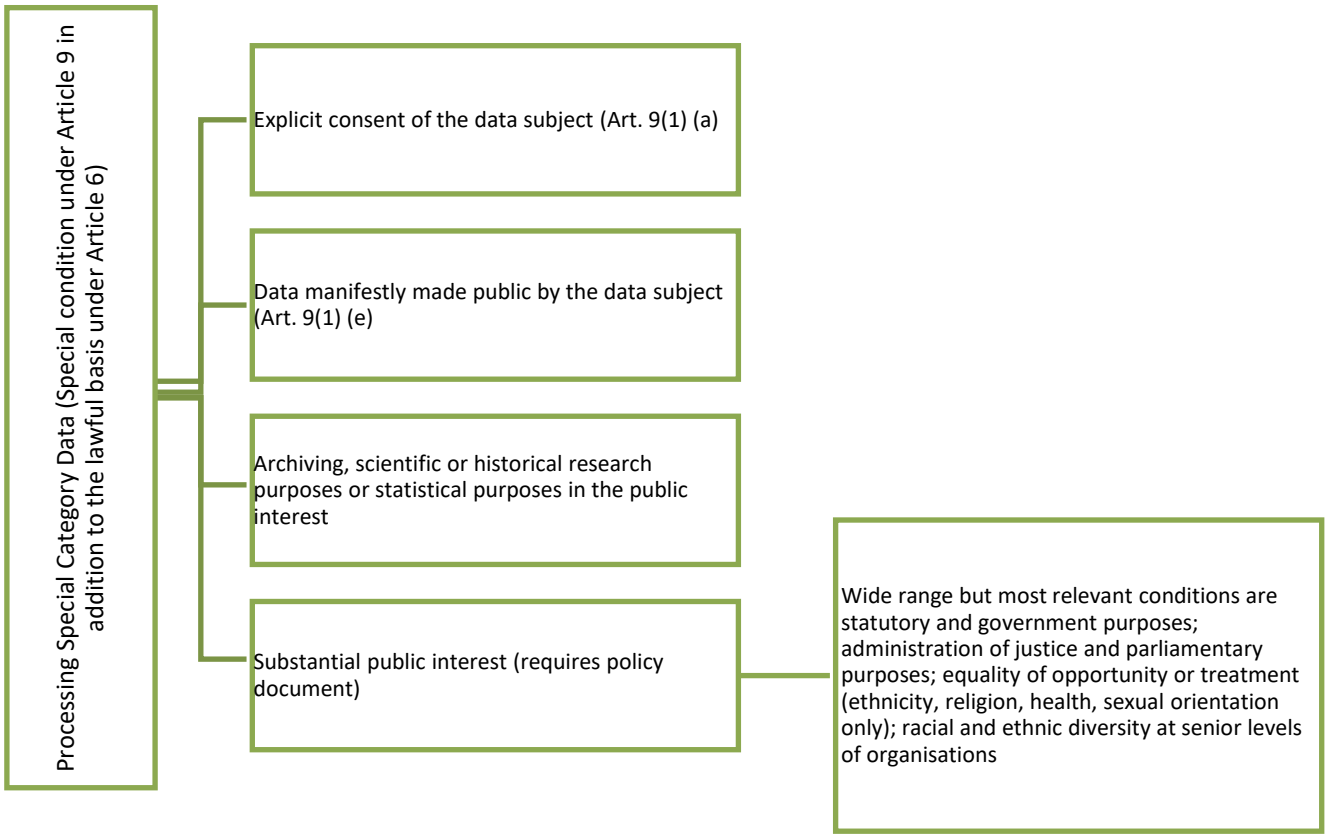
Under Schedule 1 of the DPA, if special category data is processed under substantial public interest, then you must develop policy documentation that can be made available to the ICO. The documentation must:

- Explain how the controller complies with the data protection principles
- Set out retention and erasure policies
- Be kept for at least six months after cessation of processing

[20] Article 9 GDPR; Sched. 1 DPA.

Figure 6 Main special category data processing conditions relevant for social research

(Article 9 GDPR; Section 9 and Sched. 1 DPA 2018)



13.1 Explicit consent

Explicit consent can be used a processing condition for:

- Collecting special category data or criminal offences or convictions data[21]
- Automated decision-making and/or profiling with legal or significant effects
- International data transfers to countries outside the EEA that are not deemed adequate by the EU[22]

Explicit consent must be given by a very clear and specific statement. Different options are available to provide evidence. For example, 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. [23]

If you are using explicit consent to collect special category data or criminal convictions data as a core part of a research project you must ensure that you obtain and record a specific statement such as 'Name/Signature/Date agrees to take part in this research study which will collect data about my physical health and religious beliefs and attitudes.'

If consent is the lawful ground for processing, the data subject must be able to withdraw that consent at any time. There is no exception to this requirement for scientific research. As a general rule, if consent is withdrawn, the controller must stop the processing actions and, unless there is another lawful basis for the retention of those data for further processing, the controller should delete the data.

13.2 Data made public

This condition covers personal data that the individual has made public.

There is a difference between assenting to or being aware of publication, and an individual actively making information available. You should be cautious about using this condition to justify your use of special category data obtained from social media posts.

Once you start processing this data you become the controller for the data and this condition does not exempt you from your other obligations under the GDPR.

[21] DPA 2018 Sed. 1 Part 3 (para 29) provides for standard consent rather than explicit consent for criminal convictions offences and data.

[22] See the EC website for a list of these countries: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[23] See further A29 WP guidelines on consent: 20180416_Article 29 WP Guidelines on Consent_publish.pdf .

You also need to respect an individual's rights and tell them that you are processing their data. There is no automatic exemption from transparency obligations just because information is in the public domain.

See the ICO website for more details:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/#conditions10

13.3 Substantial public interest

Under Article 9(2)(g) of the GDPR, special category data can be processed if processing is necessary for reasons of substantial public interest, and occurs on the basis of a law that is, inter alia, proportionate to the aim pursued and protects the rights of data subjects.

The DPA 2018 gives an extensive list of activities that meet substantial public interest. In a research context, the most important conditions are likely to be use for equal opportunity monitoring, examining racial and ethnic diversity at senior levels of organisations, and promoting democratic engagement. You do not have to establish a separate public interest as these categories are presumed to be in the public interest.

13.4 Processing for historical, archival, scientific or statistical research

Under Article 9(2)(j) of the GDPR special category data can be processed if necessary for archiving purposes in the public interest, for historical or scientific research or statistical purposes, subject to safeguards.

DPA 2018 Schedule 1 Part 1 para 4states that this condition is met if the processing:

- Is necessary for archiving purposes, scientific or historical research purposes or statistical purposes
- Is carried out in accordance with Article 89(1) of the GDPR (as supplemented by Section 19)
- Is in the public interest (in the general sense described in Section 11 – not of 'substantial public interest' noted in 13.3 above)

14 GLOSSARY OF TERMS AND CONCEPTS

Anonymisation

Anonymisation is the process of making personal data anonymous data. As noted in Recital 26 of the GDPR, anonymous data is 'information which does not relate to an identified or identifiable natural person or to data rendered anonymous in such a way that the data subject is not or no longer identifiable.' It is no longer personal data, and the data protection rules do not apply. However, it is increasingly difficult to properly anonymise personal data. Focus is generally placed not on the absolute impossibility of identification but the likelihood of re-identification occurring. In determining whether the data has been anonymised, consideration must be given to 'all the reasonable means likely to be used' by a motivated intruder i.e. someone seeking to reverse the anonymisation taking into account factors such as cost, available technology and amount of time it would take to reverse the de-identification of the personal data.

Controller

Controllers determine the purposes and means of processing personal data. The concept of joint controllers is formally recognised in the GDPR and applies when controllers jointly determine the purposes and means.

Criminal convictions and offences data

Under Section 11 of the DPA this is personal data relating to the alleged commission of offences by an individual, proceedings for an offence committed or alleged to have been committed by an individual, or the disposal of such proceedings including sentencing.[24]

Data protection impact assessment (DPIA)

A DPIA is a process designed to help organisations identify and mitigate data protection risks of a project. Certain high-risk processing activities require that a DPIA is carried out. The ICO website has a useful description.

Data subjects

Data subjects are identified or identifiable living individuals to whom the personal data that is held relates (Recital 26 GDPR).

[24] Article 10 GDPR; Sched. 1 DPA.

Personal data

Personal data is information relating to an identified or identifiable natural person who can be identified directly or indirectly by that data on its own or together with other data. This includes identifiers such as a name, an identification number, location data, device identifiers, cookie IDs, IP addresses and relates to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person (Article 4 GDPR).

To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by a data controller or by any other person to identify an individual directly or indirectly (Article 4 GDPR).

Personal data breach

Personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (Article 4(12) GDPR).

Processors

Processors process personal data on behalf of controller(s). In a research context an organisation is likely to be a processor if it is processing personal data solely on the client's behalf such as transcribing, processing, coding, analysing and translating activities.

Processing

Processing means any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collecting, recording, organising, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing or destroying (Article 4(2) GDPR).

Profiling

Profiling means any form of automated processing of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health or personal preferences.

Pseudonymisation

Pseudonymisation is processing personal data so that it can no longer be attributed to a specific data subject without additional information, such as a unique identifier, which can make the data identifiable. In contrast to anonymous data, pseudonymous data is personal data. In order to become pseudonymised data:

- The unique identifier must be kept separately and held subject to adequate technical and organisational measures
- Data can be considered as pseudonymised even if the unique identifier is kept within the same organisation. If the holder of the pseudonymised data does not have the means to reverse or unlock the pseudonymisation, then the data that they hold will be anonymised rather than pseudonymised data. However, this depends on the context and will be determined according to the circumstances that determine identifiability of the data

The GDPR envisages that pseudonymised data will be the default in research projects**.**

Public authority

Public authority under the DPA 2018 is as defined by the FOIA 2000, the FOIA (Scotland) 2002 and any authority or body specified by the Secretary of State in Regulations. This includes broad categories including government departments, legislative bodies and the armed forces; local government; National Health Service; maintained state schools and further and higher education institutions such as universities; police; and other named public bodies. Within the GDPR there is no definition of a public authority.

Special category data

Personal data categorised as special category data is data on religious or philosophical beliefs, health, racial or ethnic origin, trade union membership, political beliefs, sex life or sexual orientation, genetic data and biometric data (including photos when used to uniquely identify a natural person) of data subjects.[25]

Collecting and using special category data is subject to greater restrictions than other types of personal data. There needs to be a processing condition in addition to a lawful basis, and considerations of risk must be taken full account of in processing personal data. The level of risk is likely to be higher for a research project collecting special category data as the core of the project compared to limited use of data for demographic classification purposes.

[25] Article 9 GDPR; Sched. 1 DPA.

15 FREQUENTLY ASKED QUESTIONS

What is the difference between the General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 (DPA)?

The GDPR, which has direct effect across all EU Member States, came fully into effect on 25 May 2018 setting out the data protection framework across the EU.

The DPA which also came into effect on 25 May 2018 sets out the UK position for aspects in which countries are allowed to diverge from the GDPR. These include the conditions for processing special category data, and the age of children accessing online information society services[26]. It also sets out requirements for processing personal data in other areas such as law enforcement.

GDPR introduces the concept of 'privacy by design and default'. What does this mean for social research projects?

It means that all research projects involving the processing of personal data or special category data must be proactively designed and conceptualised in the most privacy enhancing way. This needs to be done by embedding privacy in organisational practices, policies and procedures.

You need to put safeguards in place, and identify privacy issues at the project planning stage to protect data. Some aspects to consider are:

- Pseudonymisation
- Data minimisation
- Storage limitation
- Access restrictions
- Retention periods
- Technical solutions such as encryption
- Organisational measures such as GDPR compliant policies and procedures and conduct of DPIAs to determine level of risk in projects

It is also best practice to develop joint data plans with clients so that the flows of personal data are fully understood, including when, if at all, personal level data is shared between client/agency and agency/client. This also helps establish data controller roles and responsibilities.

[26] Explained on the ICO website: https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/services-covered-by-this-code/

What information needs to be provided to research participants when using consent as a lawful basis for processing their personal data?

You must provide research participants with all the information they need to make choices about the collection and retention of their personal data. You can use different techniques and formats to request consent for data collection. 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.

The minimum level of information that you must provide for getting consent in a research project includes:

- Data controller(s) identity and contact details
- Details of the research supplier/s and the client (if they acting as joint controllers)
- Purpose of each processing activity that consent is being sought for e.g. for participation in research; for re-contact; for use of photos or videos
- Type of data to be collected and used
- Existence of the right to withdraw consent;
- Possible risks of data transfers to third countries outside the EEA in the absence of an adequacy decision or safeguards

You must provide this information before getting consent. You should include it on an information sheet, consent form or in the script being read to participants when seeking verbal consent for their participation.

Researchers should also seek to use effective layering of the information (see Section 4.3) to provide transparent information to participants. Information should be provided on a separate information sheet and consent form to reduce the risk of information overload and ensure that information is appropriately provided.

Even if 'consent' is not being used as the lawful basis, researchers must follow professional ethical guidance to ensure that participants understand what they are consenting to and what will happen to their data.

Can I use 'opt-out' consent for processing research data e.g. sending out standard letters to a sample frame, provided by a client, to ask people to opt out if they do not want their details passed on to a research agency?

If you are using consent as a lawful basis, then consent must be opt-in, that is, freely-given, specific, informed and unambiguous by clear affirmative action or statement.

You need to consider carefully whether another lawful basis is more appropriate than consent, such as public task or legitimate interests of the organisation (noting that legitimate interests cannot be used by public authorities in the performance of their core tasks).

What do we need to do to re-contact participants, if we have re-contact consents gained pre-GDPR?

It may be possible to use another lawful base such as public task as the basis for the re-contact. You should make sure that you meet the privacy principles of the GDPR and that the re-contact is in line with participant expectations.

How specific does consent have to be? Do researchers have to provide a detailed overview of the research purpose when getting consent?

If you are collecting personal data for scientific research purposes, and you are not able to fully specify your precise purposes in advance, you can provide a more general research purpose. If you are doing so, you need to identify the general areas of research, and if possible, give the participants detailed options that allow them to consent to certain areas of research or parts of research projects only.

You need to ensure that the project meets the interpretation of scientific research purposes. Under the GDPR this is interpreted broadly as 'including for example technological development and demonstration, fundamental research, applied research and privately funded research'. In addition, it should take into account the EU's objective under Article 179(1) TFEU of achieving a European research area, to encourage research across the EU to support innovation, medical/science/technology advancements and ensure the EU remains competitive in world markets.

What is the most appropriate processing ground for longitudinal studies conducted by university staff teams?

If longitudinal studies are being carried out by public authorities, the most likely lawful basis for processing personal data is public task. This lawful basis can be satisfied if processing is necessary (reasonable and proportionate) for carrying out a public task laid down in law. This includes university charters as well as other statutes. If you are using public task as the lawful basis, you must document this and justify it by reference to the statutory public research purpose.

Studies using personal data should, as a matter of course, also be reviewed by the relevant ethics committee.

How can research be lawfully carried out with children in educational settings such as in schools?

Research with children must be carried out in full recognition of the fact that they require particular protection as they may be less aware of the risks involved in the research. You must pay greater attention to transparency and accountability. This is especially relevant if they are using online services.

The GDPR does not define the age of a child. It sets out the age that a child can consent to online services. In the UK, the DPA 2018 sets this as a child aged 13 and over. If you wish to carry out online research with a child under the age of 13 using consent as your lawful basis then you need to get consent from the holder of parental responsibility. Best practice is to get consent from the child and parent.

If you are carrying out other types of research then you need to consider the competence of the child (that is if they have the capacity to understand the implications of you collecting and processing their personal data). If they do have this capacity, then they are competent to give their own consent for processing, unless it is evident that they are acting against their own best interests.

You can use other lawful bases, such as public task or legitimate interest, for research with children.

You should follow ethical codes which may have different and higher requirements. The MRS Code of Conduct sets the age of a child, across all channels, as a person under the age of 16. In these cases, you must seek consent from the responsible adult.

If you are carrying out research with children and young people, then you need, in all cases, to ensure that materials such as the privacy notice or consent form are tailored for the audience.

Which data subject rights does the GDPR introduce, and how will they impact on my research?

Rights of data subjects include:

- Right to be informed
- Right to access data
- Right to rectification of data
- Right to erasure or 'to be forgotten'
- Right to port data
- Right to object to processing
- Right to object to decisions taken by automated means
- Right to restrict processing

Some of these rights depend on the lawful base used for processing the data. For example, although research participants have a right to withdraw their consent or object to the processing of their data, if the research exemption applies then there are exceptions to some of these rights. For example:

- Exempt from rectification if likely to render research impossible or to seriously impair achievement of research objectives
- Exempt from restriction of processing if likely to render research impossible or to seriously impair achievement of research objectives
- Exempt from informed if personal data obtained from a third party and likely to render research impossible or to seriously impair achievement of research objectives or disproportionate resources required
- Exempt from access if likely to render research impossible or to seriously impair achievement of research objectives, and research results will not to be published in an identifiable form
- Exempt from erasure if likely to render research impossible or to seriously impair achievement of research objectives, and consent is not lawful basis
- Exempt from objection if likely to render research impossible or to seriously impair achievement of research objectives, and lawful basis is 'public interest' or data controller can show that processing is necessary to support a task carried out in the public interest

You should:

- Ensure individuals are provided with the privacy notice at the point of data capture to meet the right to information and transparency requirements
- Communicate data subject access rights and all other rights clearly to individuals in the privacy notice
- Think about how you would facilitate rectification requests during a research project and whether rectification would be appropriate given the nature of your study

Once you are holding personal data the rights are applicable.

16 FURTHER RESOURCES

- MRS GDPR FAQ: https://www.mrs.org.uk/standards/gdpr-faq
- ICO Guide to FOIA https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/
- ICO Guide to the GDPR: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/
- UK Statistics Authority Guidance on the GDPR: https://gss.civilservice.gov.uk/policy-store/uk-statistics-authority-guidance-on-the-general-data-protection-regulation-gdpr/
- National Archives Guide to archiving personal data http://www.nationalarchives.gov.uk/documents/information-management/guide-to-archiving-personal-data.pdf
- UKRI GDPR and Research: an overview for researchers: https://www.ukri.org/files/about/policy/ukri-gdpr-faqs-pdf/
- Health Research Authority Data Subject Rights and Research Exemptions: https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-detailed-guidance/data-subject-rights-and-research-exemptions/
- Scott Summers (2018). The General Data Protection Regulation (GDPR): Research and Archiving FAQs. UK Data Service, UK Data Archive. https://www.ukdataservice.ac.uk/media/621794/gdpr-faqs.pdf